

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-173285

(P2004-173285A)

(43) 公開日 平成16年6月17日 (2004.6.17)

(51) Int. Cl. 7

F I

テーマコード (参考)

H04L 9/32

H04L 9/00

673A

5B085

G06F 15/00

G06F 15/00

330B

5J104

G09C 1/00

G09C 1/00

640E

H04L 9/16

H04L 9/00

643

審査請求 未請求 請求項の数 47 O L (全 36 頁)

(21) 出願番号 特願2003-391491 (P2003-391491)
 (22) 出願日 平成15年11月20日 (2003.11.20)
 (31) 優先権主張番号 60/428,152
 (32) 優先日 平成14年11月20日 (2002.11.20)
 (33) 優先権主張国 米国 (US)
 (31) 優先権主張番号 10/459,863
 (32) 優先日 平成15年6月12日 (2003.6.12)
 (33) 優先権主張国 米国 (US)

(71) 出願人 391055833
 マイクロソフト コーポレーション
 MICROSOFT CORPORATI
 ON
 アメリカ合衆国 ワシントン州 9805
 2-6399 レッドモンド ワン マイ
 クロソフト ウェイ (番地なし)
 (74) 代理人 100077481
 弁理士 谷 義一
 (74) 代理人 100088915
 弁理士 岡部 和夫
 (72) 発明者 ショーン デリク ブレースウェル
 アメリカ合衆国 98019 ワシントン
 州 ドボル 284 サークル ノースイ
 ースト 14008

最終頁に続く

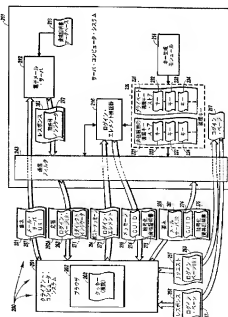
(54) 【発明の名称】 リソースへのウェブ・ベースのアクセスに使用されるクライアントの資格証明書の安全な処理

(37) 【要約】

【課題】 リソースへのウェブ・ベースのアクセスに使用されるクライアントの資格証明書の安全な処理を提供すること。

【解決手段】 ユーザの資格証明書を入力するインターフェースを有するログイン・ページがクライアントで提示され、入力されたユーザの資格証明書がサーバに送信される。ユーザの資格証明書の受信に呼応して、サーバはクライアントに対する一意のセッションIDを生成する。サーバはまた循環鍵ストアの現在の鍵と一意のセッションIDとに基づいてユーザの資格証明書に対するデジタル署名を導出する。次いでサーバは現在の鍵と一意のセッションIDから導出された暗号鍵に基づいてデジタル署名とユーザの資格証明書を暗号化する。暗号化された資格証明書がクライアントに返信されると、循環鍵ストアの鍵を使用して資格証明書の有効性確認を試みる。ユーザの資格証明書の有効性が確認不可であると、ユーザには再びログイン・ページが提示される。

【選択図】 図2A



【特許請求の範囲】

【請求項 1】

サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを試みるクライアント・コンピュータ・システムにおいて、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法であって

、前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第 1 の要求を送信する動作 (act) と、

前記クライアント・コンピュータ・システムが、ユーザの資格証明書を受け入れるためのインターフェースを提供するログイン・ページにリダイレクトされる動作 (act) と、

前記クライアント・コンピュータ・システムが、前記ログイン・ページを使用して、前記ユーザの資格証明書を前記サーバ・コンピュータ・システムに提出する動作 (act) と

、前記クライアント・コンピュータ・システムが、提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は、前記提出されたユーザの資格証明書の少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は、暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を受信する動作 (act) と、

前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記暗号化された情報をこの時点で含んでいる、第 2 の要求を送信する動作 (act) と

を備えることを特徴とする方法。

【請求項 2】

前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第 1 の要求を送信する前記動作 (act) は、以前に受信した暗号化された情報と以前に受信した一意のセッション ID とを送信する動作 (act) を備えることを特徴とする請求項 1 に記載の方法。

【請求項 3】

前記クライアント・コンピュータ・システムが前記ログイン・ページにリダイレクトされる前記動作 (act) は、前記サーバ・コンピュータ・システムによって前記以前に受信した暗号化された情報が有効であるとされなかった結果、前記クライアント・コンピュータ・システムが前記ログイン・ページにリダイレクトされる動作 (act) を備えることを特徴とする請求項 2 に記載の方法。

【請求項 4】

前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第 1 の要求を送信する前記動作 (act) は、電子メール・サーバの電子メール・リソースへのウェブ・ベースのアクセスを求める HTTP メッセージを送信する動作 (act) を備えることを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記クライアント・コンピュータ・システムが、前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報を受信する前記動作 (act) は、前記暗号化された情報を一意のセッション ID と共に受信する動作 (act) を備えることを特徴とする請求項 1 に記載の方法。

【請求項 6】

前記受信した暗号化された情報と前記受信した一意のセッション ID とを前記クライアント・コンピュータ・システムの対応するクッキーに記憶する動作 (act) をさらに備えることを特徴とする請求項 5 に記載の方法。

【請求項 7】

前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのア

10

20

30

40

50

クセスを求める第2の要求を送信する前記動作 (act) は、前記暗号化された情報を一意のセッションIDと共に送信する動作 (act) を備えることを特徴とする請求項1に記載の方法。

【請求項8】

前記クライアント・コンピュータ・システムが、前記ログイン・ページを使用して、ユーザの資格証明書を前記サーバ・コンピュータ・システムに提出する前記動作 (act) は、前記クライアント・コンピュータ・システムが、前記ログイン・ページを使用して、ユーザの資格証明書を安全な相互に認証された接続を介して前記サーバ・コンピュータ・システムに提出する動作 (act) を備えることを特徴とする請求項1に記載の方法。

【請求項9】

サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求をクライアント・コンピュータ・システムから受信する前記サーバ・コンピュータ・システムにおいて、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法であって、

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信された第1の要求を受信する動作 (act) と、

前記サーバ・コンピュータ・システムが、前記第1の要求に呼応して、前記クライアント・コンピュータ・システムがユーザの資格証明書を入力することのできるログイン・ページに、前記クライアント・コンピュータ・システムをリダイレクトする動作 (act) と

、
前記サーバ・コンピュータ・システムが、前記ログイン・ページで提出されたユーザの資格証明書を受信する動作 (act) と、

前記サーバ・コンピュータ・システムが、前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は、前記ユーザの提出した資格証明書の少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は、暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を送信する動作 (act) と、

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信され、前記暗号化された情報を含んでいる、第2の要求を受信する動作 (act) と
を備えることを特徴とする方法。

【請求項10】

前記サーバ・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを求める第1の要求を受信する前記動作 (act) は、以前に生成された暗号化された情報と以前に生成された一意のセッションIDとを受信する動作 (act) を備えることを特徴とする請求項9に記載の方法。

【請求項11】

前記サーバ・コンピュータ・システムが前記第1の要求に呼応してログイン・ページに前記クライアント・コンピュータ・システムをリダイレクトする前記動作 (act) は、以前に生成された前記暗号化された情報が前記サーバ・コンピュータ・システムによって有効であるとされなかった結果、前記サーバ・コンピュータ・システムが前記クライアント・コンピュータ・システムをログイン・ページにリダイレクトする動作 (act) を備えることを特徴とする請求項9に記載の方法。

【請求項12】

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第1の要求を受信する前記動作 (act) は、電子メール・サーバの電子メール・リソースへのウェブ・ベースのアクセスを求めるHTTPメッセージを受信する動作 (act) を備えることを特徴とする請求項9に記載の方法。

10

20

30

40

50

【請求項 13】

前記サーバ・コンピュータ・システムが、前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報を送信する前記動作 (act) は、前記暗号化された情報を一意のセッション ID と共に送信する動作 (act) を備えることを特徴とする請求項 9 に記載の方法。

【請求項 14】

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第 2 の要求を受信する前記動作 (act) は、前記暗号化された情報を一意のセッション ID と共に受信する動作 (act) を備えることを特徴とする請求項 9 に記載の方法。

10

【請求項 15】

前記クライアント・コンピュータ・システムから、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を受信するサーバ・コンピュータ・システムにおいて、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法であって、

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムによって送信された第 1 の要求を受信する動作 (act) と、

前記クライアント側の資格証明書がリソースへの無許可のアクセスを悪意のあるユーザに提供する可能性を低減するように、循環鍵ストアからの鍵を使用して前記クライアント側の資格証明書をセキュリティ保護する動作 (act) と、

20

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信された、暗号化された情報を含んでいる、第 2 の要求を受信する動作 (act) と

を備えることを特徴とする方法。

【請求項 16】

クライアント・コンピュータ・システムにおいて、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスのために使用されるユーザの資格証明書を維持する方法であって、

前記クライアント・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを求める要求であって、前記要求は、一意のセッション ID とユーザの資格証明書の少なくとも一部および時間依存署名を表す暗号化された情報とを含み、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記要求を送信する動作 (act) と、

30

前記ユーザの資格証明書の前記少なくとも一部とリフレッシュされた時間依存署名とを表すリフレッシュされた暗号化された情報であって、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部とリフレッシュされた署名時間依存鍵とから導出されており、前記暗号化された情報は、リフレッシュされた暗号化された時間依存鍵を使用して暗号化され、前記リフレッシュされた署名時間依存鍵と前記リフレッシュされた暗号化された時間依存鍵は両方とも循環鍵ストアの最新の鍵から引き出されている、前記リフレッシュされた暗号化された情報と更新された一意のセッション ID とともに前記要求されたリソースを、前記クライアント・コンピュータ・システムがクライアント側のブラウザで受信する動作 (act) と、

40

前記クライアント・コンピュータ・システムが、前記更新されたセッション ID と前記リフレッシュされた暗号化された情報とをクライアント・コンピュータ・システムの対応するクッキーに記憶する動作 (act) と

を備えることを特徴とする方法。

【請求項 17】

50

前記クライアント・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを求める要求を送信する前記動作 (act) は、電子メール・サーバの電子メール・リソースへのウェブ・ベースのアクセスを求める H T T P メッセージを送信する動作 (act) を備えることを特徴とする請求項 16 に記載の方法。

【請求項 18】

前記クライアント・コンピュータ・システムが、前記要求されたリソースを更新された一意のセッション I D とリフレッシュされた暗号化された情報と共にクライアント側のブラウザで受信する前記動作 (act) は、前記暗号化された情報の生成で使用されている鍵が循環鍵ストアの前記最新の鍵でないということに起因して、更新されたセッション I D とリフレッシュされた暗号化された情報とを受信する動作 (act) を備えることを特徴とする請求項 16 に記載の方法。

10

【請求項 19】

前記クライアント・コンピュータ・システムが、前記更新された一意のセッション I D と前記リフレッシュされた暗号化された情報とを前記クライアント・コンピュータ・システムの対応するクッキーに記憶する前記動作 (act) は、前記一意のセッション I D と前記リフレッシュされた暗号化された情報をブラウザ・メモリ内の前記一意のセッション I D と暗号化された情報に書き出す動作 (act) を備えることを特徴とする請求項 16 に記載の方法。

【請求項 20】

サーバ・コンピュータ・システムで、前記サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスに使用されるユーザの資格証明書の有効性を決定する方法において、

20

前記サーバ・コンピュータ・システムが、前記サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求であって、前記要求は、一意のセッション I D と、前記ユーザの資格証明書の少なくとも一部および時間依存署名を表す暗号化された情報とを含み、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記要求を受信する動作 (act) と、

前記サーバ・コンピュータ・システムが、循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の少なくとも一部の有効性確認を試みる動作 (act) と、

30

前記サーバ・コンピュータ・システムが、前記要求されたリソースへのウェブ・ベースのアクセスを制御するモジュールに前記要求を転送する動作 (act) と、

前記サーバ・コンピュータ・システムが、前記ユーザの資格証明書の前記少なくとも一部と前記時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきか否かを判定する動作 (act) と

を備えることを特徴とする方法。

【請求項 21】

前記循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の少なくとも一部の有効性確認を試みる前記動作 (act) は、前記循環鍵ストアの前記最新の鍵に基づいて前記ユーザの資格証明書の前記少なくとも一部が有効であると判定する動作 (act) を備えることを特徴とする請求項 20 に記載の方法。

40

【請求項 22】

前記循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の前記少なくとも一部の有効性確認を試みる前記動作 (act) は、前記循環鍵ストアの前記最新の鍵に基づいて前記ユーザの資格証明書の前記少なくとも一部が有効でないかと判定する動作 (act) を備えることを特徴とする請求項 20 に記載の方法。

【請求項 23】

前記サーバ・コンピュータ・システムが、前記循環鍵ストア内の以前に生成された鍵で前記循環鍵ストア内に前記最新の鍵よりも前に挿入された鍵、に基づいて前記ユーザの資

50

格証明書の前記少なくとも一部が有効であると判定する動作 (act) をさらに備えることを特徴とする請求項 20 に記載の方法。

【請求項 24】

前記サーバ・コンピュータ・システムが、前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきかを判定する前記動作 (act) は、前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきであると判定する動作 (act) を備えることを特徴とする請求項 20 に記載の方法。

【請求項 25】

前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきであると判定する前記動作 (act) は、前記サーバ・コンピュータ・システムが、前記循環鍵ストア内の以前に生成された鍵で、前記循環鍵ストア内に最新の鍵より前に挿入された鍵、に基づいて前記ユーザの資格証明書の少なくとも一部を有効であると判定する動作 (act) を備えることを特徴とする請求項 24 に記載の方法。

【請求項 26】

前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報とが前記循環鍵ストアの前記最新の鍵から導出されるべきであると判定する前記動作 (act) は、前記サーバ・コンピュータ・システムが、前記循環鍵ストア内のいかなる鍵によっても前記ユーザの資格証明書の前記少なくとも一部を有効であるとなることができなかつたと判定する動作 (act) を備えることを特徴とする請求項 24 に記載の方法。

【請求項 27】

前記サーバ・コンピュータ・システムは、ユーザの資格証明書を受信するためのインターフェースを提供するログイン・ページに前記クライアント・コンピュータ・システムをリダイレクトする動作をさらに備えることを特徴とする請求項 26 に記載の方法。

【請求項 28】

前記サーバ・コンピュータ・システムが、前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されているかを判定する前記動作 (act) は、リフレッシュされた暗号化された情報と時間依存署名とを前記循環鍵ストアの前記最新の鍵から導出する動作 (act) を備えることを特徴とする請求項 20 に記載の方法。

【請求項 29】

前記サーバ・コンピュータ・システムは、前記要求されたリソースと前記更新された一意のセッション ID とリフレッシュされた暗号化された情報とを前記クライアント・コンピュータ・システムに送信する動作 (act) をさらに備えることを特徴とする請求項 28 に記載の方法。

【請求項 30】

メッセージ・ヘッダーを変更することができる通信フィルタを含むサーバ・コンピュータ・システムにおいて、クライアント・コンピュータ・システムに関連付けられた通信プロパティを決定する方法において、

H T T P メッセージの処理方法を変更することのできる 1 つまたは複数の選択可能な通信プロパティを選択するためのインターフェースを含むログイン・ページを前記クライアント・コンピュータ・システムに送信する動作 (act) と、

前記ログイン・ページから選択可能な前記 1 つまたは複数の選択可能な通信プロパティで、前記クライアント・コンピュータ・システムとの H T T P 通信の処理方法を前記通信フィルタに指示する通信プロパティ、の少なくとも 1 つの選択を受信する動作 (act) と

前記受信した少なくとも 1 つの通信プロパティ選択がサポートされているかを判定

10

20

30

40

50

するため、また前記クライアント・コンピュータ・システムがサポートする他の関連通信プロパティを特定するために、前記クライアント・コンピュータ・システムに問い合わせる動作 (act) と、

任意の選択された通信プロパティと前記クライアント・コンピュータ・システムがサポートする特定された他の関連通信プロパティとに従って前記クライアント・コンピュータ・システムとの H T T P 通信を処理するように前記通信フィルタを構成する動作 (act) と

を備えることを特徴とする方法。

【請求項 3 1】

前記ログイン・ページから選択可能な前記 1 つまたは複数の選択可能な通信プロパティの少なくとも 1 つの選択を受信する前記動作 (act) は、前記クライアント・コンピュータ・システムの信頼性を指示する通信プロパティ選択を受信する動作 (act) を備えることを特徴とする請求項 3 0 に記載の方法。 10

【請求項 3 2】

前記ログイン・ページから選択可能な前記 1 つまたは複数の選択可能な通信プロパティの少なくとも 1 つの選択を受信する前記動作 (act) は、前記クライアント・コンピュータ・システムのコンテンツ処理能力および/または所望の機能レベルを指示する通信プロパティ選択を受信する動作 (act) を備えることを特徴とする請求項 3 0 に記載の方法。

【請求項 3 3】

前記クライアント・コンピュータ・システムに問い合わせる前記動作 (act) は、前記クライアント・コンピュータ・システムが H T T P 圧縮をサポートすると決定する動作 (act) を備えることを特徴とする請求項 3 0 に記載の方法。 20

【請求項 3 4】

クライアント・コンピュータ・システムにおいて、サーバ・コンピュータ・システムに求められる通信プロパティを指示する方法であって、

前記サーバによる H T T P メッセージの処理方法を変更することができる 1 つまたは複数の選択可能な通信プロパティを選択するためのインターフェースを含むログイン・ページをサーバ・コンピュータ・システムから受信する動作 (act) と、

前記クライアント・コンピュータ・システムで前記ログイン・ページを提示する動作 (act) と、 30

前記ログイン・ページで前記 1 つまたは複数の通信プロパティの少なくとも 1 つの選択を受信する動作 (act) と、

前記クライアント・コンピュータ・システムとの H T T P 通信の処理方法を通信フィルタに指示する前記通信プロパティ選択を前記サーバ・コンピュータ・システムの前記通信フィルタに送信する動作 (act) と

を備えることを特徴とする方法。

【請求項 3 5】

前記ログイン・ページで前記 1 つまたは複数の通信プロパティの少なくとも 1 つの選択を受信する前記動作は、前記クライアント・コンピュータ・システムの信頼性を示す選択を受信する動作 (act) を備えることを特徴とする請求項 3 4 に記載の方法。 40

【請求項 3 6】

前記ログイン・ページで前記 1 つまたは複数の通信プロパティの少なくとも 1 つの選択を受信する前記動作 (act) は、前記クライアント・コンピュータ・システムのコンテンツ処理能力および/または所望の機能レベルを指示する選択を受信する動作 (act) を備えることを特徴とする請求項 3 4 に記載の方法。

【請求項 3 7】

前記通信プロパティ選択を前記サーバ・コンピュータ・システムの通信フィルタに送信する前記動作 (act) は、前記通信プロパティ選択をユーザの資格証明書と共に送信する動作 (act) を備えることを特徴とする請求項 3 4 に記載の方法。

【請求項 3 8】

サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを試みるクライアント・コンピュータ・システムで使用するための、前記リソースへのアクセスが許可されるために使用されるクライアント側の資格証明書をセキュリティ保護する方法を実装するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記クライアント・コンピュータ・システムに、

前記リソースへのウェブ・ベースのアクセスを求める第1の要求を送信すること、

ユーザの資格証明書を受け入れるためのインターフェースを提供するログイン・ページにリダイレクトされること、

前記ログイン・ページを使用して、前記サーバ・コンピュータ・システムにユーザの資格証明書を提出すること、

前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵とは両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を受信すること、および

前記リソースへのウェブ・ベースのアクセスを求める、前記暗号化された情報をこの時点で含む、第2の要求を送信すること

を実行させるコンピュータ実行可能命令を記憶している1つまたは複数のコンピュータ可読媒体を備えることを特徴とするコンピュータ・プログラム製品。

【請求項39】

前記1つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項38に記載のコンピュータ・プログラム製品。

【請求項40】

クライアント・コンピュータ・システムから、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を受信するサーバ・コンピュータ・システムで使用するための、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法を実施するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記サーバ・コンピュータ・システムに、

前記クライアント・コンピュータ・システムによって送信された、前記リソースへのウェブ・ベースのアクセスを求める第1の要求を受信すること、

前記第1の要求に呼応して、前記クライアント・コンピュータ・システムがユーザの資格証明書を入力することのできるログイン・ページに前記クライアント・コンピュータ・システムをリダイレクトすること、

前記ログイン・ページで提出された前記ユーザの資格証明書を受信すること、

前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵とは両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を受信すること、および

前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信された、前記暗号化された情報を含む、第2の要求を受信することを実行させるコンピュータ実行可能命令を記憶している1つまたは複数のコンピュータ可読媒体を備えるコンピュータ・プログラム製品。

【請求項41】

前記1つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項40に記載のコンピュータ・プログラム製品。

【請求項42】

サーバ・コンピュータ・システムで使用するための、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスのために使用されるユーザの資格証明書の有効

10

20

30

40

50

性を決定する方法を実装するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記サーバ・コンピュータ・システムに、

前記サーバ・コンピュータ・システムの前記リソースへのウェブ・ベースへのアクセスを求める、一意のセッションIDと、ユーザの資格証明書の少なくとも一部および時間依存署名を表す暗号化された情報とを含む要求であって、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されていること、

前記循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の前記少なくとも一部の有効性確認を試みること、

前記要求されたリソースへのウェブ・ベースのアクセスを制御するモジュールに前記要求を転送すること、および

前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されているか否かを判定すること

を実行させるコンピュータ実行可能命令を記憶している1つまたは複数のコンピュータ可読媒体を備えることを特徴とするコンピュータ・プログラム製品。

【請求項43】

前記1つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項42に記載のコンピュータ・プログラム製品。

【請求項44】

メッセージ・ヘッダーを変更することができる通信フィルタを含むサーバ・コンピュータ・システムで使用するための、クライアント・コンピュータ・システムに関連付けられた通信プロパティを決定する方法を実装するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記サーバ・コンピュータ・システムに、HTTPメッセージの処理方法を変更することのできる1つまたは複数の選択可能な通信プロパティを選択するためのインターフェースを含むログイン・ページを前記クライアント・コンピュータ・システムに送信すること、

前記ログイン・ページから選択可能な前記1つまたは複数の選択可能な通信プロパティで、前記クライアント・コンピュータ・システムとのHTTP通信の処理方法を前記通信フィルタに示すプロパティ、の少なくとも1つの選択を受信すること、

前記受信した少なくとも1つの通信プロパティ選択がサポートされているか否かを判定するため、また前記クライアント・コンピュータ・システムがサポートする他の関連通信プロパティを特定するために、前記クライアント・コンピュータ・システムに問い合わせること、

任意の選択された通信プロパティと前記クライアント・コンピュータ・システムがサポートする特定された他の関連通信プロパティとに従って前記クライアント・コンピュータ・システムとのHTTP通信を処理するように前記通信フィルタを構成すること

を実行させるコンピュータ実行可能命令を記憶している1つまたは複数のコンピュータ可読媒体を備えることを特徴とするコンピュータ・プログラム製品。

【請求項45】

前記1つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項44に記載のコンピュータ・プログラム製品。

【請求項46】

HTTPメッセージをフィルタリングするよう構成されたサーバ・コンピュータ・システムであって、

1つまたは複数の処理装置と、

1つまたは複数のコンピュータ可読媒体であって、

HTTPメッセージを受信し、

前記HTTPメッセージに含まれる一意のセッションIDに基づいて前記HTTPメッ

10

20

30

40

50

セージを送信したクライアント・コンピュータ・システムを特定し、

前記クライアント・コンピュータ・システムに関連付けられたクライアントの状態情報にアクセスし、

ユーザの資格証明書と時間依存署名とを表す暗号化された情報の有効性確認を試み、前記クライアントの状態情報で示された通信プロパティに基づいて前記H T T Pメッセージが変更されるべきか否かを判定する

ように構成されている1つまたは複数のコンピュータ可読媒体とを備えることを特徴とするサーバ・コンピュータ・システム。

【請求項47】

リソースへのウェブ・ベースのアクセスのための資格証明情報を安全に表記するための10
のフォーマットを規定するデータ構造を記憶している1つまたは複数のコンピュータ可読媒体であって、前記データ構造は、

前記リソースへのウェブ・ベースのアクセスを制御するモジュールで認証するためのユーザの資格証明書を表記する資格証明書フィールドと、

前記モジュールと前記資格証明書フィールドに表されている前記ユーザの資格証明書を提出したクライアント・コンピュータ・システムとの間でH T T Pメッセージを転送する場合に使用されるべき1つまたは複数の通信プロパティを表記するフラグ・フィールドと

、
前記資格証明書フィールドに表されている前記ユーザの資格証明書と前記フラグ・フィールドに表されている前記通信プロパティとを有効性確認するために使用することができ20
る時間依存デジタル署名を表すハッシュ・メッセージ認証コード・フィールドとを備えることを特徴とする1つまたは複数のコンピュータ可読媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、コンピュータ・ネットワークに関し、より詳細には、リソースに対するウェブ・ベースのアクセスに使用されるクライアントの資格証明書(credential)を安全に処理することに関する。

【背景技術】

【0002】

30
コンピュータ・システムおよび関連技術は、社会の多くの側面に影響を与える。実際、情報を処理するコンピュータ・システムの機能は、我々の生活および仕事の方法に変化を与えてきた。現在、コンピュータ・システムは、一般に、コンピュータ・システムが出現する前には手作業で行われていた多くの作業(例えば、文書処理、スケジューリング、およびデータベース管理)を実行している。さらに最近では、コンピュータ・システムは相互に結合されて、コンピュータ・システムが有線と無線のコンピュータ・ネットワークの両方構成し、それを介してコンピュータ・システムが電子的に通信し、データを共有することができるようになった。その結果、コンピュータ・システムで実行される多くのタスク(例えば、音声通信、電子メールへのアクセス、電子会議、ウェブ・ブラウジング)40
には、1つまたは複数の他のコンピュータ・システムとの無線および/または有線コンピュータ・ネットワークを介した電子通信が含まれている。

【0003】

特に、電子メールは、通信のための重要な方法になった。電子メールのシステムは、通常、電子メール・クライアント装置と電子メール・サーバ装置とを含む。これらの装置は、通常、コンピュータ・システム(例えば、サーバ、P C、ラップトップ、およびP D A)上で実行されるように構成されたソフトウェア・アプリケーションである。電子メール・クライアント装置と電子メール・サーバ装置は、通常、相互の特定動作作用に設計・構成されている。電子メール・クライアント装置と電子メール・サーバ装置は、一般に、例えばクライアント・コンピュータ・システムのアプリケーション・プログラムがサーバ・コンピュータ・システム上のプログラムを実行することを可能にする、リモート・プロシー50

ジャ・コール（「RPC: Remote Procedure Calls」）のような独自開発のプロトコルを使用して相互に通信する。例えば、電子メール・クライアント装置は、電子メール・サーバ装置に適切な引数によってメッセージを送信することができ、電子メール・サーバ装置は電子メール・メッセージを返信する。

【0004】

電子メール・サーバの一部の種類は、専用電子メール・クライアントではなく、例えばウェブ・ブラウザを有するクライアント・コンピュータ・システムのような「ゼロタッチ（zero-touch）」クライアントを介して電子メールにアクセスできるよう構成されている。これらの種類の電子メール・サーバでは、ウェブ・ブラウザは電子メール・サーバと対話し、クライアントシステム上で実行することが必要な機能ならばどのような機能でもウェブ・ブラウザを介して実行される。例えば、クライアント・コンピュータ・システムは、ウェブ・ブラウザが電子メール・サーバと適切に対話することを可能にするハイパー・テキスト・マークアップ言語（「HTML」）命令とスクリプト（アクティブ・サーバ・ページのような技術によって動的に生成される）をダウンロードすることができる。すなわち、ゼロタッチのブラウザ・ベースのクライアントは、ユーザが、自分の電子メールと、ゼロタッチのブラウザ・ベースのクライアントによって共通ネットワーク（例えば、ワールドワイドウェブ（「WWW」））に接続されている任意のサーバ・コンピュータ・システムからの他のメール関連情報（例えば、カレンダーおよび共用フォルダ）とにアクセスすることを可能にする。したがって、例えばWWW上のウェブ・ベースのコンテンツにアクセスするために使用されるハイパー・テキスト転送プロトコル（「HTTP」）のようなプロトコルを、電子メールおよび他のメール関連情報にアクセスするために使用することもできる。

【0005】

しかし、電子メールおよび他のメール関連情報へのブラウザ・ベースのアクセス可能性は潜在的なセキュリティ問題をもたらし、いくつかのセキュリティ問題はウェブ・ブラウザ・メモリ内のユーザの資格証明書のキャッシングに関連している。ウェブ環境において、コンテンツおよびコンテンツに対する要求（request）は、一般にHTTPを使用して配送される。例えば、コンテンツへのアクセスを求めるHTTP要求がブラウザ・ベースのクライアントのユーザからネットワークに向けて配送される。次いで要求はサーバ・コンピュータ・システムのウェブ・サーバで受信され、そこでその要求を処理して要求したコンテンツにアクセスすることをブラウザ・ベースのクライアントのユーザが許可されているか否かを判定する。ユーザが要求したコンテンツにアクセスすることを許可されている場合、ウェブ・サーバはコンテンツをHTTPメッセージでブラウザ・ベースのクライアントに返信する。

【0006】

HTTPの一部のバージョン（例えば、HTTP/1.0）はステートレス（stateless）である。すなわち、HTTPを介した通信（例えば、電子メール・メッセージの要求）は、サーバによる以前のいかなる通信に関する知識（例えば、電子メール・メッセージに対する他の以前の要求）なしに実行される。したがって、HTTPのこれらのバージョンは、ユーザが「ログイン」または「ログアウト」する「セッション」の概念をサポートしない。HTTPの他のバージョン（例えば、HTTP/1.1）は、HTTP接続を継続状態（alive）に保つよう試みるためにクライアントとサーバの間で送信される「キープアライブ（keep-alive）」メッセージをサポートする。しかし、キープアライブ・メッセージの使用は、やや信頼性に乏しく、キープアライブ・メッセージが使用される場合であっても、HTTP接続がアクティブに保たれる保証はない。さらに、クライアントの要求が複数のユーザ間でキープアライブ・リンクを共用する中間プロキシ・サーバを介して頻繁に送り込まれるので、受信した要求が以前に認証されたクライアントによって送信されたか否かをサーバが判定することはない。したがって、HTTP接続がステートレスか、またはキープアライブ・メッセージを使用しているかに関わらず、HTTPを介して配送されるコンテンツへのアクセスを求める各要求（以下、「HTTP要求」と呼ぶ）は、

10

20

30

40

50

適切な HTTP 認証情報 (authentication information) を含む必要がある。

【0007】

したがって、HTTP 認証情報は、WWW-許可 (Authorization) ヘッダーと呼ばれ、「WWW-許可: [認証タイプ] [資格証明書 (Credentials)]」というフォーマットを有する特別なヘッダーを介して HTTP 要求に含めることができる。ウェブ・ブラウザが最初に認証を必要とするコンテンツ (例えば、ユーザが入力した資格証明書の提出) へのアクセスを試みると、ウェブ・サーバは、通常、要求されたコンテンツを提供することを拒否し、代わりにステータス・コード 401「無許可 (Unauthorized)」を有する HTTP メッセージを返信する。この HTTP 応答 (response) メッセージには、「WWW-認証 (Authenticate): [認証方法] [領域=領域値] [任意選択情報]」というフォーマットのヘッダーが含まれる。

10

【0008】

ウェブ・ブラウザで返信を受信すると、HTTP 応答メッセージは、ウェブ・ブラウザに、例えばユーザ名およびパスワードのような資格証明書を要求するダイアログボックスを提示させる。ユーザが資格証明書を入力した後、ウェブ・ブラウザは、元の HTTP 要求を、入力された資格証明書を含む HTTP WWW-認証ヘッダーと共に再送する。ウェブ・サーバが、ユーザの入力した資格証明書を有効であるとして受け入れて、要求されたコンテンツ (例えば、電子メール・メッセージ) を返信した場合、ウェブ・ブラウザは、ユーザが入力した資格証明書をブラウザのメモリにキャッシュする。したがって、同じユーフォーム・リソース・ロケータ (URL) または同じコンテンツに関連付けられた対応する派生的な関連 URL へのそれ以降の要求では、キャッシュされた資格証明書がブラウザのメモリから取り出され、対応する HTTP WWW-許可ヘッダーに含められる。この結果、HTTP がステートレスであっても、ユーザは、同じまたは対応する派生的な関連 URL に対するそれぞれの要求について資格証明書を再入力する必要から、開放される。

20

【発明の開示】

【発明が解決しようとする課題】

【0009】

残念ながら、ウェブ・ブラウザは、一般に、(ウェブブラウザプログラムを終了する (quitting) か、またはコンピュータ・システムまたはクライアントのデバイスを再起動 (re-booting) またはターン・オフすることによって) ウェブ・ブラウザが終了されるまで、キャッシュされた資格証明書を基本的に無期限でブラウザのメモリに保持する。したがって、保護されたコンテンツにアクセスした特権のあるユーザの資格証明書は、そのユーザがそのウェブ・ブラウザを使用しなくなった後もブラウザのメモリにキャッシュされている可能性がある。次いで特権のあるユーザがコンピュータ・システムのそばを離れた場合、別の特権のないユーザがやってきて、ブラウザの戻りボタンまたは履歴機能を使用して保護されたコンテンツへのアクセスを試みる可能性がある。特権のあるユーザの資格証明書がブラウザのメモリに依然としてキャッシュされているので、ウェブ・ブラウザは、キャッシュされた資格証明書を取り出し、それらを保護されたコンテンツにアクセスする特権のないユーザの要求と共に提出する。したがって、特権のないユーザが、ウェブ・ブラウザで適切な資格証明書を入力することを必要とせずに、保護されたコンテンツへのアクセスを得る可能性がある。

30

40

【0010】

キャッシュされた資格証明書は、ウェブ・ブラウザを終了することを許可しない公共のコンピュータおよび/またはコンピュータ・システムのある場所では特に問題となり得る。そのようなコンピュータ・システムの一例としてインターネット・キオスクがある。インターネット・キオスクは、一般大衆にインターネットへのアクセスを提供するために、例えば図書館、インターネットカフェ、および会議センターのような公共の場所に置かれることがしばしばある。インターネット・キオスクは、キオスクのある場所に来た人なら誰でも、最初にウェブ・ブラウザを探して起動することを必要とせずに迅速にインターネ

50

ットにアクセスすることを可能にするよう設計されている。したがって、多くのインターネット・キオスクは、ウェブ・ブラウザが常時活動状態にあり終了されることがないように構成されている。

【0011】

この結果、インターネットへの効率的なアクセスが提供されるが、またキャッシュされた資格証明書が基本的に無期限でブラウザのメモリに残存することにもなる。例えば特権のあるユーザが（例えば、保護されたコンテンツにアクセスするために）インターネット・キオスクに資格証明書を入力する場合、その特権のあるユーザの資格証明書はブラウザのメモリにキャッシュされる。ウェブ・ブラウザは終了されるはずがないので、その公共のキオスクの電源を切らずにキャッシュされた資格証明書を除去する方法は基本的にない。したがって、特権のあるユーザがキャッシュされた資格証明書を消す方法を知っていたとしても（例えば、ウェブ・ブラウザを終了することによって）、特権のあるユーザがそれを実行することから、防止されているかもしれない。

10

【0012】

保護されたコンテンツにアクセスするためにキャッシュされた資格証明書を使用することは、ブラウザ・ベースの電子メールアプリケーションにとって特別重要な問題である。例えば、特権のないユーザは、ページを戻して個人的なデータを含んでいる可能性のある特権のあるユーザの電子メール・メッセージにアクセスすることができる。特権のあるユーザの電子メールにアクセスすることに加え、キャッシュされた資格証明書は特権のないユーザが特権のあるユーザになりますことを可能にする場合もある。例えば、特権のないユーザは、特権のあるユーザに関連付けられたアカウントから電子メール・メッセージを送信することができる場合がある。

20

【0013】

この問題に対する1つの可能な解決法は、コンテンツが要求されるたびにユーザに再認証を強制することである。しかしこれにより、ユーザはコンテンツにアクセスするHTTP要求ごとに認証情報を手動で再入力することが要求される。ウェブ・サイトとの通常の対話は数十または場合によっては数百のHTTP要求から構成される場合があるので、ユーザは数十回、または数百回も資格証明書を再入力しなければならないことになる。したがって、HTTP要求ごとに資格証明書を再入力することは、コンテンツにアクセスするために必要な時間とデータ入力の量を大幅に増加させることになる。この解決法は多くのユーザにとってあまりにも煩雑すぎ、ユーザは、1回のセッションに自分の資格証明書を1回だけ入力することを好む。したがって、ウェブ・ベースのリソースへのアクセスに使用されるクライアントの資格証明書を安全に処理するシステム、方法、コンピュータ・プログラム製品が有利になるであろう。

30

【課題を解決するための手段】

【0014】

従来技術における前述の問題は、本発明の原理によって解決され、本発明の原理は、リソースへのウェブ・ベースのアクセスのために使用されるクライアントの資格証明書を安全に処理する方法、システム、コンピュータ・プログラム製品、およびデータ構造に向けられている。クライアント・コンピュータ・システム（以下、「クライアント」と呼ぶ）と、サーバ・コンピュータ・システム（以下、「サーバ」と呼ぶ）は、例えばインターネットのような共通のネットワークに接続されている。サーバは、例えば電子メール・メッセージおよび関連するメール・データのようなリソースへのウェブ・ベースのアクセスを可能にするように構成されている。クライアントは、ウェブ・ベースのリソースへのアクセスを要求し、ウェブ・ベースのリソースをそのクライアントのユーザに提示することのできる、ブラウザを含んで構成されている。

40

【0015】

クライアントは、サーバのリソースにアクセスすることを求める第1の要求を送信する。例えば、クライアントは、サーバに記憶されている電子メール・メッセージへのアクセスを要求する要求を送信することができる。サーバは第1の要求を受信するが、クライ

50

トが無許可であるため、サーバは第1の要求の受信に呼応してそのクライアントをログイン・ページにリダイレクトする。クライアントをリダイレクトすることは、サーバがクライアントに、ログイン・ページへのユニフォーム・リソースID (Identifier) (「URI」) と共にリダイレクション・インジケータ (例えば、ステータス・コード302「一時移動」) を有するハイパー・テキスト転送プロトコル (「HTTP」) メッセージを含む応答を送信することを含むことができる。このログイン・ページは、クライアントのユーザがユーザの資格証明書を入力するためのインターフェースを提供するアクティブ・サーバ・ページ (「ASP」) ページであってよい。クライアントはこのログイン・ページにアクセスし、そのログイン・ページを使用してユーザの資格証明書をサーバに提出する。クライアントは、例えばHTTPポストをセキュリティ保護するためにセキュア・ソケット・レイヤ (「SSL」) を使用して、資格証明書を提出することができる。

10

【0016】

サーバは提出された資格証明書を受信する。サーバは、ユーザの資格証明書と時間依存デジタル署名を表す暗号化された情報を送信する。サーバは、認証を実行する信頼された機関に、提出された資格証明書についての認証を委任した後、暗号化された情報を送信する場合がある。サーバは、循環鍵ストア (rotating key store) の鍵を使用して暗号化されたデータを生成する。循環鍵ストアの各鍵は指定時間間隔 (例えば10分) 後に自動的に期限が切れる。指定時間間隔後、サーバは循環鍵ストア内に新しい鍵を循環させ、期限切れの鍵を循環鍵ストアから取り外すように循環させることができる。循環鍵ストアで保持される鍵の数と指定時間間隔は管理者が構成することができる。

20

【0017】

ユーザの資格証明書が受信されると、サーバはユーザの資格証明書を一意識別子 (例えば、グローバル一意識別子 (「GUID」)) に関連付ける。サーバは、循環鍵ストアの最新の鍵と一意識別子と第1の定数列との組み合わせを (例えば、SHA-1またはMD-5 ハッシング・アルゴリズムを使用して) ハッシュすることによって、データにデジタル的に署名するために使用することができる。署名鍵を導出する。次いでサーバは、この署名鍵を使用して、一意識別子とユーザの資格証明書の組み合わせからデジタル署名 (例えば、ハッシュ・メッセージ認証コード (「HMAC」)) を導出する。

【0018】

サーバは、データを暗号化するために使用することのできる暗号鍵も、循環鍵ストアの最新の鍵と一意識別子と第2の定数列との組み合わせをハッシュすることによって、導出する。次いでサーバは、この暗号鍵を使用して、デジタル署名とユーザの資格証明書の組み合わせを、暗号化された情報の中に暗号化する。サーバは、一意識別子と暗号化された情報とをクライアントに送信する。クライアントは、この一意識別子と暗号化された情報を受信し、一意識別子と暗号化された情報を (例えば対応するクッキーに) 格納する。

30

【0019】

クライアントは、サーバのリソースへのアクセスを求める、一意識別子と暗号化された情報を含む第2の要求を送信する。サーバは、第2の要求を受信し、循環鍵ストア中の最新の鍵を使用してユーザの資格証明書の有効性確認を試みる。サーバは、循環鍵ストアの最新の鍵と一意識別子と第2の定数列との組み合わせをハッシュすることによって、データを暗号解読するために使用することのできる、暗号解読鍵を導出する。サーバは、暗号解読鍵を使用して暗号化された情報を暗号解読し、それによってデジタル署名とユーザの資格証明書を明らかにする (平文にする)。サーバは、循環鍵ストアの最新の鍵と一意識別子と第1の定数列との組み合わせとをハッシュすることによって、データを認証するために使用することのできる、有効性確認鍵を導出する。サーバは、有効性確認署名鍵を使用して、一意識別子とユーザの資格証明書の組み合わせから有効性確認デジタル署名を導出する。

40

【0020】

サーバは、有効性確認デジタル署名をデジタル署名と比較する。有効性確認デジタル署名とデジタル署名が一致した場合、ユーザの資格証明書は有効であるとされる。一方、有

50

効性確認デジタル署名とデジタル署名が一致しない場合、資格証明書は有効であるとされない。ユーザの資格証明書が、循環鍵ストアの最新の鍵を使用して有効であるとされない場合、循環鍵ストア内で次の最も新しい鍵が使用され（例えば、次の最も新しい鍵を使用して暗号解読鍵と有効性確認デジタル署名を生成することにより）、ユーザの資格証明書の有効性確認が試みられる。サーバは、循環鍵ストアの各鍵を使用してユーザの資格証明書の有効性確認を試みることができる。有効であるとされたユーザの資格証明書は、要求されたリソース（例えば、電子メール・メッセージ）へのアクセスを制御するモジュール（例えば、電子メール・サーバ）に転送される。

【0021】

ユーザの資格証明書が、循環鍵ストアの最新の鍵ではない鍵によって有効であるとされた場合、サーバはリフレッシュされた暗号化された情報を導出すべきであると判定する。サーバは、循環鍵ストアの最新の鍵を使用して、（例えば、リフレッシュされたデジタル署名とリフレッシュされた暗号鍵を最新の鍵から導出することにより）リフレッシュされた暗号化された情報を導出する。有効であるとされたユーザの資格証明書が適切である場合、要求されたリソースが、リフレッシュされた暗号化された情報を適宜ともなってクライアントに返信される。クライアントは、リソースと任意のリフレッシュされた暗号化された情報を受信する。クライアントは、任意のリフレッシュされた暗号化された情報で一意識別子に対応する以前に暗号化された情報を上書きして記憶する。ユーザの資格証明書が循環鍵ストアのいかなる循環鍵を使用しても有効であるとして行うことができない場合、クライアントは、新しいユーザの資格証明書を入力することができるログイン・ページにリダイレクトされる。

【0022】

いくつかの実施形態では、ログイン・ページはHTTPメッセージの処理方法を変更することができる通信プロパティ（例えば、gzip圧縮に対するサポートについて、クライアント・コンピュータ・システムがプライベートであるかまたは信頼性のないクライアントであるかについて、クライアントが簡素化したコンテンツを好む上級のクライアントであることについてのプロパティ）を選択するためのインターフェースを含む。通信プロパティはログイン・ページで選択され、クライアントとのHTTP通信の処理方法を通信フィルタに示すために通信フィルタに送信される。選択された通信プロパティがサーバで受信される。

【0023】

サーバは、選択された通信プロパティをクライアントがサポートしているか否かを判定するため、また他の関連通信プロパティを特定するため、クライアントに問い合わせる。サーバは、任意の選択された通信プロパティとクライアントがサポートすると特定された他の関連通信プロパティに従ってクライアントとのHTTP通信を処理するよう通信フィルタを構成する。クライアントが安全でない場所にいるということに基づいて、サーバは、循環間隔が短く、より少数の鍵を保持する別の循環鍵ストアを使用することができる。

【0024】

本発明のさらなる機能および利点は、以下の説明で述べることで、また一部は以下の説明から明らかになろうし、あるいは本発明を実施することによって知ることができよう。本発明の機能および利点は、特に特許請求の範囲で指摘された機器および組み合わせを使用して実現し、得ることができる。本発明のこれらおよび他の機能は、以下の説明および特許請求の範囲からより完全に明らかになろうし、また以下で述べるように本発明を実現することによって知ることができよう。

【発明を実施するための最良の形態】

【0025】

本発明の上記および他の利点および機能を得ることができる方法を説明するために、上記で概説した本発明のより具体的な説明が、添付の図面に示す本発明の具体的な実施形態を参照することによって提供される。これらの図面は本発明の典型的な実施形態だけを示しており、したがって本発明の範囲を限定するものとみなされるべきではないということ

を理解して、本発明は、添付の図面を使用してさらなる特殊性および詳細を以って記載し説明される。

【0026】

本発明の原理は、リソースに対するウェブ・ベースのアクセスのために使用されるクライアントの資格証明書の安全な処理を提供する。サーバは、1つまたは複数の鍵のうち少なくとも1つの循環鍵ストアを保持する。循環鍵ストア中の各鍵は指定時間間隔（例えば10分）後に自動的に有効期限が切れる。指定時間間隔後、サーバは循環鍵ストア内部に循環新しい鍵を循環させ、循環期限切れの鍵を循環鍵ストアから取り外すように循環させる。循環鍵ストアで保持される鍵の数と指定時間間隔は管理者が構成することができる（例えば、3つの鍵を保持して5分ごとに鍵を循環する）。サーバは、ユーザの資格証明書に対するデジタル署名を生成し、循環鍵ストアの鍵に基づいてユーザの資格証明書を暗号化することによってユーザの資格証明書をセキュリティ保護する。

10

【0027】

ユーザの資格証明書を入力するためのインターフェースを有するログイン・ページがクライアントで提示される。クライアントで入力されたユーザの資格証明書はサーバに送信される。ユーザの資格証明書の受信に呼応して、サーバはクライアントに対する一意のセッションIDを生成する。サーバは、循環鍵ストアの最新の鍵と一意のセッションIDに基づいてユーザの資格証明書に対するデジタル署名を導出する。次いでサーバは、循環鍵ストアの最新の鍵と一意のセッションIDから導出した暗号鍵に基づいてデジタル署名とユーザの資格証明書を暗号化する。暗号化された資格証明書がクライアントに返信されると、循環鍵ストアからの鍵が使用されて、資格証明書の有効性確認を試みられる。ユーザの資格証明書を暗号化するために元々使用された循環鍵ストアからの鍵が、循環鍵ストアから取り外すように循環すると、クライアントは、新しい資格証明書を入力するためのログイン・ページにリダイレクトされる。

20

【0028】

本発明の範囲にある実施形態は、コンピュータ実行可能命令を搬送し、またはデータ構造を格納するためのコンピュータ可読媒体を含む。このようなコンピュータ可読媒体は、汎用または専用コンピュータ・システムによってアクセス可能な任意の人手可能な媒体であってよい。限定ではなく一例として、このようなコンピュータ可読媒体は、RAM、ROM、EPROM、CD-ROMまたは他の光ディスク・ストレージ、磁気ディスク・ストレージまたは他の磁気記憶装置、または所望のプログラム・コード手段をコンピュータ実行可能命令、コンピュータ可読命令、またはデータ構造の形式で搬送または記憶するために使用することができ、汎用または専用コンピュータ・システムによってアクセスすることができ、いかなる他の媒体でも含むことができる。

30

【0029】

本明細書および特許請求の範囲では、「ネットワーク」をコンピュータ・システムおよび/またはモジュール間で電子データの転送を可能にする1つまたは複数のデータリンクと定義する。情報がネットワークまたは他の通信接続（ハード・ワイヤード、無線、またはハード・ワイヤードと無線の組み合わせのどれか）を介してコンピュータ・システムに送信すなわち提供される場合、接続はコンピュータ可読媒体と厳密にみなされる。したがって、このような接続はいつでも厳密にはコンピュータ可読媒体と呼ばれる。上記の組み合わせもコンピュータ可読媒体の範囲に含まれるべきである。コンピュータ実行可能命令は、例えば汎用コンピュータ・システムまたは専用コンピュータ・システムに特定の関数または一群の関数を実行させる命令およびデータを含んでいる。コンピュータ実行可能命令は、例えばバイナリ、アセンブリ言語のような中間形式の命令、または場合によってはソース・コードであってよい。

40

【0030】

本明細書および首記の特許請求の範囲では、「コンピュータ・システム」を、協同して電子データに対していくつかの動作を実行する1つまたは複数のソフトウェア・モジュール、1つまたは複数のハードウェア・モジュール、またはこれらの組み合わせと定義する

50

。例えばコンピュータ・システムの定義は、パーソナル・コンピュータのハードウェア構成要素、並びにパーソナル・コンピュータのオペレーティング・システムのようなソフトウェア・モジュールを含む。モジュールの物理的レイアウトは重要ではない。コンピュータ・システムは、ネットワークを介して結合された1つまたは複数のコンピュータを含むことができる。同様に、コンピュータ・システムは、(メモリおよびプロセッサの一般的な)内部モジュールが協同して電子データに対していくつかの動作を実行する(携帯電話またはパーソナル・デジタル・アシスタント「PDA」のような)単一の物理デバイスを含むことができる。

【0031】

当業者には、本発明が、パーソナル・コンピュータ、ラップトップ・コンピュータ、ハンドヘルド装置、マルチ・プロセッサ・システム、マイクロプロセッサ・ベースの、すなわちプログラム可能な家庭用電化製品、ネットワークPC、ミニ・コンピュータ、メインフレーム・コンピュータ、携帯電話、PDA、ページなどを含めて多くのタイプのコンピュータ・システム構成を有するネットワーク・コンピューティング環境で実施することができるということが理解されよう。本発明は、(ハード・ワイヤード・データリンク、無線データリンク、またはハード・ワイヤード・データリンクと無線データリンクの組み合わせのどれかによって)ネットワークを介してリンクされたローカル・コンピュータ・システムと遠隔コンピュータ・システムがどちらもタスクを実行する分散型システム環境で実施することもできる。分散型システム環境では、プログラム・モジュールはローカル・メモリ・ストレージ・デバイスと遠隔メモリ・ストレージ・デバイスの両方に置くことができる。

【0032】

図1および以下の説明は、本発明を実装することができる適切なコンピューティング環境の簡単で一般的な説明を提供することを意図している。必ずしもこの通りである必要はないが、本発明は、コンピュータ・システムが実行しているプログラム・モジュールのようなコンピュータ実行可能命令という一般的な状況で説明する。一般に、プログラム・モジュールは、特定のタスクを実行し、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、構成要素、データ構造などを含む。データ構造に関連付けられたコンピュータ実行可能命令とプログラム・モジュールとは、本明細書で開示された方法の動作を実行するためのプログラム・コード手段の例を表している。

【0033】

図1を参照すると、本発明を実装するシステム例は、汎用コンピューティング・デバイスを、処理装置121とシステム・メモリ122と、システム・メモリ122を含む様々なシステム構成要素を処理装置121に結合するシステム・バス123とを含めてコンピュータ・システム120の形式で含む。処理装置121は、本発明の機能を含めてコンピュータ・システム120の機能を実装するように設計されたコンピュータ実行可能命令を実行することができる。システム・バス123は、メモリ・バスまたはメモリ・コントローラ、周辺バス、および様々なバス・アーキテクチャのどれかを使用するローカルバスを含めたいくつものタイプのバス構造のどれであってもよい。システム・メモリは、読取専用メモリ(「ROM」)124とランダム・アクセス・メモリ(「RAM」)125を含む。起動時などにコンピュータ・システム120内の素子間で情報を転送することに役立つ基本ルーチンを含んでいる基本入出力システム(「BIOS」)126をROM124に記憶することができる。

【0034】

コンピュータ・システム120は、磁気ハードディスク139から読み取る／に書き込むための磁気ハードディスク・ドライブ127、取り外し可能な磁気ディスク129から読み取る／に書き込むための磁気ディスク・ドライブ128、CD-ROMまたは他の光媒体のような取り外し可能な光ディスク131から読み取る／に書き込むための光ディスク・ドライブ130も含むことができる。磁気ハードディスク・ドライブ127、磁気ディスク・ドライブ128、および光ディスク・ドライブ130は、それぞれにハードディ

10

20

30

40

50

スク・インターフェース132、磁気ディスクドライブ・インターフェース133、および光ドライブ・インターフェース134によってシステム・バス123に接続される。これらドライブおよびこれらの関連するコンピュータ可読媒体は、コンピュータ・システム120に対してコンピュータ実行可能命令、データ構造、プログラム・モジュール、および他のデータの非揮発性ストレージを提供する。本明細書で説明される実施形態は磁気ハードディスク139、取り外し可能な磁気ディスク129、および取り外し可能な光ディスク131を使用しているが、磁気カセット、フラッシュ・メモリ・カード、デジタル多用ディスク、バルヌーイ・カートリッジ、RAM、ROMなどを含めてデータを記憶するための他のタイプのコンピュータ可読媒体を使用することもできる。

【0035】

1つまたは複数のプログラム・モジュールを含んでいるプログラム・コード手段は、オペレーティング・システム135、1つまたは複数のアプリケーション・プログラム136、他のプログラム・モジュール137、およびプログラム・データ138を含めて、ハードディスク139、磁気ディスク129、光ディスク131、ROM124、またはRAM125に記憶することができる。ユーザは、キーボード140、ポインティング・デバイス142、または例えばマイクロフォン、ジョイスティック、ゲームパッド、スキャナなどのような他の入力装置（図示せず）を介してコンピュータ・システム120にコマンドおよび情報を入力することができる。これらおよび他の入力装置は、システム・バス123に結合されている入出力インターフェース146を介して処理装置121に接続することができる。入出力インターフェース146は、例えばシリアル・ポート・インターフェース、PS/2インターフェース、パラレル・ポート・インターフェース、ユニバーサル・シリアル・バス（「USB」）インターフェース、または米国電気電子学会（「IEEE」）1394インターフェース（すなわち、FireWireインターフェース）のような幅広い様々な異なるインターフェースのどれでも論理的に表し、または異なるインターフェースの組み合わせを論理的に表すこととさせることができる。

【0036】

モニタ147または他の表示装置もビデオ・アダプタ148を介してシステム・バス123に接続される。スピーカー169または他の音声出力装置も、音声インターフェース149を介してシステム・バス123に接続される。例えばプリンタのような他の周辺装置（図示せず）も、コンピュータ・システム120に接続することができる。コンピュータ・システム120は、例えば事務所全体または企業全体のコンピュータ・ネットワーク、ホームネットワーク、イントラネット、および/またはインターネットのようなネットワークに接続可能である。コンピュータ・システム120は、例えば遠隔コンピュータ・システム、遠隔アプリケーション、および/または遠隔データベースのような外部ソースとそのようなネットワークを介してデータを交換することができる。

【0037】

コンピュータ・システム120は、それを介して外部ソースからデータを受信し、かつ/または外部ソースにデータを送信するネットワーク・インターフェース153を含む。図1に示すように、ネットワーク・インターフェース153は、リンク153を介した遠隔コンピュータ・システム183とのデータの交換に役立つ。ネットワーク・インターフェース153は、ネットワーク・インターフェース・カードおよび対応するネットワーク・ドライバ・インターフェース規約（「NDIS」）スタックのような1つまたは複数のソフトウェアおよび/またはハードウェア・モジュールを論理的に表すことができる。リンク151はネットワークの一部（例えば、イーサネット（登録商標）のセグメント）を表し、遠隔コンピュータ・システム183はネットワークのノードを表す。例えば遠隔コンピュータ・システム183は、コンピュータ・システム120にリソース（例えば、電子メール・メッセージ）へのウェブ・ベースのアクセスを提供するサーバ・コンピュータ・システムであってよい。一方、遠隔コンピュータ・システム183は、コンピュータ・システム120からリソースにアクセスするためにウェブ・ベースのアクセスを使用するクライアント・コンピュータ・システムであってよい。

10

20

30

40

50

【0038】

同様に、コンピュータ・システム120は、コンピュータ・システム120自体が外部ソースからデータを受信し、かつ／または外部ソースにデータを送信する入出力インターフェース146を含む。入出力インターフェース146は、コンピュータ・システム120がそれを介して外部ソースからデータを受信し、かつ／または外部ソースにデータを送信するリンク159を介してモデム154（例えば、標準モデム、ケーブルモデム、またはデジタル加入者回線（「DSL」）モデム）に結合されている。図1に示すように、入出力インターフェース146とモデム154は、リンク152を介した遠隔コンピュータ・システム193とのデータの交換に役立つ。リンク152はネットワークの一部を表し、遠隔コンピュータ・システム193はネットワークのノードを表す。例えば遠隔コンピュータ・システム193は、コンピュータ・システム120にリソース（例えば、電子メール・メッセージ）へのウェブ・ベースのアクセスを提供するサーバ・コンピュータ・システム120からリソースにアクセスするためにウェブ・ベースのアクセスを使用するクライアント・コンピュータ・システムであってよい。

10

【0039】

図1は本発明に適したオペレーティング環境を表しているが、本発明の原理は、必要に応じて適切な修正を行い本発明の原理を実装することができるどのシステムでも使用することができる。図1に示した実施形態は説明のみを目的としており、本発明の原理を実装することができる幅広い様々な環境のほんの一部さえも表すものではない。

20

【0040】

本発明のモジュール並びに関連するプログラム・データは、コンピュータ・システム120に関連付けられたコンピュータ可読媒体のどれからでも記憶し、アクセスすることができる。例えばそのようなモジュールの一部および関連するプログラム・データの一部は、システム・メモリ122での記憶用に、オペレーティング・システム135、アプリケーション・プログラム136、プログラム・モジュール137、および／またはプログラム・データ138に含めることができる。例えば磁気ハードディスク139のような大容量記憶装置がコンピュータ・システム120に結合されている場合、そのようなモジュールおよび関連するプログラム・データも大容量記憶装置に記憶することができる。ネットワーク接続された環境で、コンピュータ・システム120に関連して示されたプログラム・モジュールまたはその一部は、遠隔コンピュータ・システム183および／または遠隔コンピュータ・システム193に関連付けられたシステム・メモリおよび／または大容量記憶装置のような遠隔メモリ・ストレージ・デバイスに記憶することができる。そのようなモジュールの実行は、前述のような分散環境で実行することができる。

30

【0041】

図2Aおよび図2Bは、クライアントがサーバのリソースへのアクセスを要求する際にクライアント側の資格証明書をセキュリティ保護することに役立つネットワーク・アーキテクチャ200の一例を示している。クライアント・コンピュータ・システム201とサーバ・コンピュータ・システム211は、例えばローカル・エリア・ネットワーク（「LAN」）、ワイドエリアネットワーク（「WAN」）、または場合によってはインターネットのような共通ネットワークに接続することができる。クライアント・コンピュータ・システム201は、リソースへのウェブ・ベースのアクセスを要求し、受信したリソースをクライアント・コンピュータ・システム201で提示するために使用することのできるブラウザ202を含む。クッキー203は、サーバ・コンピュータ・システムから以前に受信したデータの一部を記憶する1つまたは複数のクッキーを含むことができる。クッキー203内のデータは、個人的な情報または好みをサーバ・コンピュータ・システムに示し、かつ／または記憶されている情報の一部を手動で入力するユーザの手間を省くために、対応するサーバ・コンピュータ・システムに送信されることがある。

40

【0042】

サーバ・コンピュータ・システム211は、例えば電子メール・メッセージ、アドレス

50

ブック情報、およびカンレンダリング情報のような電子メール・リソースへのアクセスを提供する電子メール・サーバ212を含む。電子メール・リソースにアクセスする許可を得るには、ユーザは電子メール・サーバ212によって認証するために電子メール・サーバ212に資格証明書を提供することが要求される場合がある。電子メール・サーバ212は、電子メール・リソースへのアクセスを求める要求が承諾されるべきか否かを判定するために、受信した資格証明書を資格証明書データベース213の許可された資格証明書と比較することができる。ユーザが許可されている場合、電子メール・サーバ212は、要求された電子メール・リソースを要求側のクライアント・コンピュータ・システムに返信することができる。ユーザが許可されていない場合、電子メール・サーバ212は、無許可メッセージ（例えば、ステータス・コード401「無許可」を有するハイパー・テキスト転送プロトコル（「HTTP」）メッセージ）を要求側クライアント・コンピュータ・システムに返信することができる。

10

【0043】

サーバ・コンピュータ・システム211は、鍵（キー）生成モジュール214も含むことができる。鍵生成モジュール214は、循環鍵（キー）群220に新しい鍵を生成して循環させることができ、期限切れの鍵を循環鍵群220から取り外すように循環させることができる。鍵生成モジュール214は、1つまたは複数の循環鍵ストアを保持するように構成することができる。例えばネットワーク・アーキテクチャ200で、鍵生成モジュール214は、非信頼用の循環鍵（キー）ストア221とプライベート循環鍵（キー）ストア231を保持する。

20

【0044】

鍵が循環される際の指定時間間隔は設定可能である。すなわち、指定された間隔で循環鍵ストア内に新たに生成された鍵を循環させ、期限切れになった鍵を循環鍵ストアから除去するよう鍵生成モジュール214を構成することができる。例えば、鍵生成モジュール214は、10分ごとに、新しい鍵をプライベート循環鍵ストア231に挿入し、期限切れの鍵をプライベート循環鍵ストア231から除去することができる。循環鍵ストアで保持される鍵の数も構成可能である。すなわち鍵（キー）生成モジュール214は、循環鍵ストア内に指定された数の鍵を保持するように構成することもできる。例えば、鍵生成モジュール214は、非信頼用の循環鍵ストア221内に3つの鍵を保持するように構成することができる。

30

【0045】

保持される鍵の数と指定された間隔は循環鍵ストアによって異なる場合がある。例えば、鍵生成モジュール214は、非信頼用の鍵ストア221内に5分という指定された循環間隔で3つの鍵を保持し、プライベート鍵ストア231内に1時間という指定された循環間隔で4つの鍵を保持することができる。クライアント・コンピュータ・システムに関連付けられたプロパティに応じて、本発明の原理を実装するために異なる鍵ストアを使用することができる。循環鍵ストアの鍵の下に示した矢印は、循環鍵ストアが循環して最終的に期限切れの鍵が出るまで、新しい鍵が追加されるとこれらの鍵が循環に従って送られていくことを示している。例えば、プライベート循環鍵ストア231に新しい鍵が追加されると、鍵232は循環に従って鍵233の位置に入る。

40

【0046】

サーバ・コンピュータ・システム211はログイン・ページ217も含む。ログイン・ページ217は、ユーザの資格証明書を提出し、クライアント・コンピュータ・システムに関連付けられた通信プロパティを選択するためのインターフェースを提供するウェブ・ページ（例えば、アクティブ・サーバ・ページ「ASP」ページ）であってよい。クライアント・コンピュータ・システムがログイン・ページ217に対応するユニフォーム・リソースID（「URI」）にアクセスすることに呼応して、サーバ・コンピュータ・システム211はログイン・ページ217をクライアント・コンピュータ・システムに送信することができる。クライアント側のブラウザはクライアント・コンピュータ・システムでログイン・ページ217を提示することができる。ログイン・ページ217で提出された

50

ユーザの資格証明書と通信プロパティの選択は、サーバ・コンピュータ・システム 211 に送信することができる。

【0047】

サーバ・コンピュータ・システムは通信フィルタ 243 も含む。通信フィルタ 243 は、例えばサーバ・コンピュータ・システム 211 の中へ／から外へ送信される要求、応答、およびメッセージのような HTTP 通信をインターセプト (intercept) することができる。通信フィルタ 243 は、暗号化されたクッキーに含まれるクライアント状態情報を参照して、サーバ・コンピュータ・システム 211 とクライアント・コンピュータ・システムとの間の HTTP 通信を (例えば、HTTP ヘッダーを修正することによって) 変更すべきか否かを判定することができる。通信フィルタ 243 は、循環鍵ストアの鍵を使用して) 暗号アルゴリズムを実装して、ユーザの資格証明書を暗号解読し有効性確認すること

10

【0048】

サーバ・コンピュータ・システム 211 は、ログイン要素バリデータ (validator; 検証器) 216 も含む。ログイン要素バリデータ 216 は、ログイン・ページ 217 で入力されて提出されたユーザの資格証明書を受信することができ、(循環鍵ストアの鍵を使用して) 暗号アルゴリズムを実装して、提出されたユーザの資格証明書をデジタル署名し、暗号化することができる。ログイン要素バリデータ 216 は、サーバ・コンピュータ・システム 211 のリソースへのウェブ・ベースのアクセスを要求するクライアント・コンピュータ・システムのために、一意のセッション ID (例えば、グローバル・識別子 (「GUID」)) を生成することもできる。ログイン要素バリデータ 216 は、一意のセッション ID と、ユーザの資格証明書および時間依存デジタル署名を含む暗号化された情報とをクライアント・コンピュータ・システムに送信することができる。例えば、ログイン要素バリデータ 216 は、一意のセッション ID と暗号化されたユーザの資格証明書を、クッキー 203 での記憶用にクライアント・コンピュータ・システム 201 に送信することができる。

20

【0049】

図 3 は、クライアントがサーバのリソースへのアクセスを要求する際にクライアント側の資格証明書をセキュリティ保護する方法 300 の流れ図の一例を示している。その方法 300 を、図 2A に示すクライアント・コンピュータ・システムとサーバ・コンピュータ・システムに関して説明する。方法 300 は、第 1 の要求をサーバに送信する動作 (動作 301) を含む。動作 301 は、クライアント・コンピュータ・システムが、サーバのリソース (例えば、電子メール・メッセージ) へのウェブ・ベースのアクセスを求める第 1 の要求を送信することを含むことができる。

30

【0050】

例えば、クライアント・コンピュータ・システム 201 は、メール・サーバの URI 267 を含む要求 251 をサーバ・コンピュータ・システム 211 に送信することができる。メール・サーバの URI 267 は、電子メール・サーバ 212 に対応する URI であってよい。すなわち、電子メール・サーバが保持している電子メール・リソースにアクセスすることを望むユーザは、メール・サーバの URI 267 にアクセスすることによって電子メール・リソースへのウェブ・ベースのアクセスを試みることができる。したがって、クライアント・コンピュータ・システム 201 のユーザは、クライアント・コンピュータ・システム 201 に要求 251 を送信させるようブラウザ 202 にコマンドを入力する。

40

【0051】

方法 300 は、第 1 の要求をクライアントから受信する動作 (動作 306) を含む。動作 306 は、サーバ・コンピュータ・システムが、サーバのリソース (例えば、電子メール・メッセージ) へのウェブ・ベースのアクセスを求める第 1 の要求を受信することを含むことができる。例えば、サーバ・コンピュータ・システム 211 は、メール・サーバの URI 267 を含む要求 251 をクライアント・コンピュータ・システム 201 から受信することができる。通信フィルタ 243 を通過する破線で示すように、通信フィルタ 24

50

3は要求251を変更せずに通過させることができるよう構成することができる。この結果、要求251は修正なしに電子メール・サーバ212に転送することができる。

【0052】

方法300は、クライアント側の資格証明書をセキュリティ保護する機能結果志向(functional result-oriented)のステップ(ステップ311)を含む。ステップ311は、クライアント側の資格証明書をセキュリティ保護するすべての対応する動作を含むことができる。しかし図3に示す例では、ステップ311は、第1の要求に呼応してクライアントをログイン・ページにリダイレクトする対応する動作(動作307)を含む。動作307は、第1の要求に呼応してサーバ・コンピュータ・システムがクライアント・コンピュータ・システムをログイン・ページにリダイレクトすることを含むことができる。

10

【0053】

要求251に呼応して、電子メール・サーバ212は、無許可インジケータ272を含む応答(レスポンス)252を送信することができる。応答252は、ユーザの資格証明書を含まない要求251の結果として返信されたステータス・コード401「無許可」を有するHTTPメッセージであってよい。通信フィルタ243は、無許可インジケータを含むメッセージをインターセプトするように構成することができる。この結果、通信フィルタ243は応答252をインターセプトすることができる。

【0054】

通信フィルタ243は、クライアント・コンピュータ・システム201を、ユーザの資格証明書を入力するためのインターフェースを提供するログイン・ページにリダイレクトさせるために、応答252のコンテンツを(例えば、HTTPヘッダーを変更することによって)修正することができる。例えば、通信フィルタ243は、応答252から無許可インジケータ272を除去し、ログイン・ページのURI263とリダイレクト・インジケータ271を応答252に挿入することができ、これにより応答252Aが生じる。応答252Aは、ステータス・コード302「発見」を有するHTTPメッセージであってよい。ログイン・ページのURI263は、ログイン・ページ271にアクセスするために使用されるURIであってよい。この結果、応答252Aは、要求されたリソース(例えば、電子メール・メッセージ)の代わりにログイン・ページのURI263にアクセスされるということをクライアント・コンピュータ・システム201に示すことができる。

20

【0055】

方法300は、ログイン・ページにリダイレクトされる動作(動作(act)302)を含む。動作(act)302は、クライアント・コンピュータ・システムが、ユーザの資格証明書を受け入れるためのインターフェースを提供するログイン・ページにリダイレクトされることを含むことができる。例えば、クライアント・コンピュータ・システム201はログイン・ページ217にリダイレクトすることができる。要求252Aの受信に呼応して、クライアント・コンピュータ・システム201は、ログイン・ページのURI263を含む要求(リクエスト)257をサーバ・コンピュータ・システム211に送信することができる。要求257に呼応して、サーバ・コンピュータ・システム211は、ログイン・ページ217を含む応答(レスポンス)258をクライアント・コンピュータ・システム201に送信することができる。ログイン・ページは、例えばアクティブ・サーバ・ページ(「ASP」)ページのようなウェブ・ページであってよい。

30

40

【0056】

ブラウザ202はクライアント・コンピュータ・システム201でログイン・ページ217を提示することができる。図3から移動して次に図6を参照すると、図6は、本発明の原理により、ユーザの資格証明書と通信プロパティの選択を受け入れることのできるログイン・ページの一例600を示している。ログイン・ページ217はログイン・ページ600に類似してよい。ログイン・ページ600は、ユーザIDを受け入れることのできるフィールド606と、対応するパスワードを受諾することのできるフィールド607を含む。

【0057】

50

クライアント側のブラウザが「上級のクライアント」であることを示す通信プロパティ選択を受け入れるためにラジオ・ボタン601を使用することができる。クライアント側のブラウザが「ダウン・レベル・クライアント」であることを示す通信プロパティ選択を受け入れるためにラジオ・ボタン602を使用することができる。上級クライアントは、例えばスクリプトを実行すること、またはマルチメディア出力を提示することのようなさらに高度な処理を実行する機能を含むことができる。一方、ダウン・レベル・クライアントは、高度な処理を実行する機能を含むことはできない。この結果、サーバから返信されたコンテンツの豊かさ、クライアント側のブラウザの機能に応じて適切に調整することができる。上級クライアントが短縮された帯域幅および／または長い待ち時間接続（例えば、ダイヤルアップ接続）を介してサーバに接続されている場合、ダウン・レベル・クライアントの選択はサーバから返信されるコンテンツ量を低減することができる。

10

【0058】

クライアント側のブラウザが「信頼のない（非信頼の）クライアント・コンピュータ・システム」であることを示す通信プロパティ選択を受け入れるために、ラジオ・ボタン603を使用することができる。クライアント側のブラウザが「プライベート・クライアント・コンピュータ・システム」にあることを示す通信プロパティ選択を受け入れるために、ラジオ・ボタン604を使用することができる。プライベート・クライアント・コンピュータ・システムは、公共アクセス（public access）が限定された（あるいはまったくない）家庭用または企業用のクライアント・コンピュータ・システムであってよい。「信頼のないクライアント・コンピュータ・システム」は、例えばホテルまたは空港のインターネット・キオスクのようなさらに多くの公共アクセスを有するクライアント・コンピュータ・システムであってよい。この結果、サーバから返信されたコンテンツに関連付けられたセキュリティは、クライアント・コンピュータ・システムの信頼性に適切に調整することができる。入力されたユーザの資格証明書と選択された通信プロパティをサーバ・コンピュータ・システムに送信するためにボタン608を選択することができる。

20

【0059】

図6から移動して次に図5を参照すると、図5は、本発明の原理により、クライアントに関連付けられた通信プロパティを決定するための方法500の流れ図の一例を示している。方法500は、ネットワーク・アーキテクチャ200に示すクライアント・コンピュータ・システムとサーバ・コンピュータ・システムに関して示す。方法500は、ログイン・ページをクライアントに送信する動作（act）（動作（act）501）を含む。動作501は、サーバ・コンピュータ・システムが、HTTPメッセージの処理方法を変更することができる1つまたは複数の通信プロパティを選択するためのインターフェースを含むログイン・ページを送信することを含むことができる。例えば、サーバ・コンピュータ・システム211は、ログイン・ページ600（または類似のログインページ）をクライアント・コンピュータ・システム201に送信することができる。

30

【0060】

方法500は、サーバからログイン・ページを受信する動作（動作505）を含む。動作500は、クライアント・コンピュータ・システムが、サーバによるHTTPメッセージの処理方法を変更することができる1つまたは複数の通信プロパティを選択するためのインターフェースを含むログイン・ページを受信することを含むことができる。例えば、クライアント・コンピュータ・システム201はログイン・ページ600（または類似のログインページ）を受信することができる。方法500は、クライアントでログイン・ページを提示する動作（動作506）を含む。動作506は、クライアント・コンピュータ・システムのブラウザがクライアント・コンピュータ・システムでログイン・ページを提示することを含むことができる。例えば、ブラウザ202は、クライアント・コンピュータ・システム201でログイン・ページ600（または類似のログイン・ページ）を提示することができる。

40

【0061】

方法500は、1つまたは複数の通信プロパティの少なくとも1つで選択を受信する動

50

作（動作507）を含む。動作507は、クライアント・コンピュータ・システムが、ログイン・ページで1つまたは複数の通信プロパティの少なくとも1つの選択を受け取ることを含むことができる。例えば、ユーザはクライアント・コンピュータ・システム201で、ログイン・ページ600に通信プロパティ選択を入力するために入力装置（例えば、キーボードおよび／またはマウス）を操作することができる。ログイン・ページ600は、ユーザが入力した選択を受け取ることができる。例えば、ログイン・ページ600は、ラジオ・ボタン601またはラジオ・ボタン602のユーザが入力した選択、およびラジオ・ボタン603またはラジオ・ボタン604のユーザが入力した選択を受け取ることができる（場合によっては、フィールド606および607でユーザが入力した資格証明書の受け取りと共に）。

10

【0062】

方法500は、サーバの通信フィルタに通信プロパティ選択を送信する動作（動作508）を含む。動作508は、クライアント・コンピュータ・システムが、サーバ・コンピュータ・システムの通信フィルタに通信プロパティ選択を送信することを含むことができる。例えば、クライアント・コンピュータ・システム201は、サーバ・コンピュータ・システム211に通信プロパティ選択（例えば、ユーザが入力した資格証明書と共に）を送信することができる。方法500は、クライアントから少なくとも1つの通信プロパティ選択を受信する動作（動作502）を含む。動作502は、サーバ・コンピュータ・システムがログイン・ページから選択可能な1つまたは複数の選択可能な通信プロパティの少なくとも1つの選択を受信することを含むことができる。例えば、通信フィルタ243は、クライアント・コンピュータ・システム201から（例えば、ログイン・ページ600で選択された）1つまたは複数の通信プロパティ選択を受信することができる。

20

【0063】

方法500は、受信した少なくとも1つの通信プロパティ選択がサポートされているかを判定するために、またクライアントがサポートする他の関連通信プロパティを特定するために、クライアントに問い合わせる動作（動作503）を含む。動作503は、サーバ・コンピュータ・システムが、受信した通信プロパティ選択がサポートされているかを判定するため、またクライアントがサポートする他の関連通信プロパティを特定するために、クライアント・コンピュータ・システムに問い合わせることを含むことができる。例えば、サーバ・コンピュータ・システムは、ユーザーエージェントのHTTPヘッダーとクライアント・コンピュータ・システムの以前の知識を使用してクライアント・コンピュータ・システムの機能を決定することができる。クライアント・コンピュータ・システムの追加の機能は、ログイン・ページを介して、またクライアント・コンピュータ・システムのログイン・ページ内で実行されているスクリプト（例えば、Java（登録商標）Scriptのスクリプト）から、決定することができる。

30

【0064】

別法として、クライアント・コンピュータ・システムに対する問い合わせは、クライアント・コンピュータ・システムに構成情報をサーバ・コンピュータ・システムに対して明らかにさせる要求をクライアント・コンピュータ・システムに送信することを含むことができる。例えば、サーバ・コンピュータ・システム211は、ブラウザ202の構成を求める要求をクライアント・コンピュータ・システム201に送信することができる。これに呼応して、ブラウザ202は、例えば、バージョン番号とブラウザ202がgzip圧縮のようなHTTP圧縮をサポートするかのような構成情報を示すことができる。バージョン番号に基づいて、サーバ・コンピュータ・システム211は、ログイン・ページ600での「上級クライアント」の選択が適切であったか否かを判定することができる。例えば、サーバ・コンピュータ・システムは、ブラウザ202のバージョンがスクリプトをサポートしないか判定することができる場合がある。したがって、「上級クライアント」が選択された場合でも、サーバ・コンピュータ・システムは、簡素化したコンテンツをクライアント・コンピュータ・システム201に提供することができる。

40

【0065】

50

コンテンツを簡素化することは、クライアント・コンピュータ・システムに配信されるコンテンツの量を低減することを含むことができる。例えば、ヘルプ情報に対するダウン・レベル・クライアント要求に呼応して、サーバ・コンピュータ・システムは、縮小した（冗長でない）ヘルプ情報を返信することができる。一方、ヘルプ情報に対する上級クライアント要求に呼応して、サーバ・コンピュータ・システムは、より充実させたヘルプ情報、例えば、検索スクリプトおよび他の拡張機能を含む情報を返信することができる。サーバ・コンピュータ・システムは、クライアント・コンピュータ・システムの信頼性に基づいて配信されたコンテンツを変更することができる。例えば、サーバ・コンピュータ・システムは、機密に関わる企業データへのアクセス方法に関するヘルプ情報をプライベート・クライアント・コンピュータシステムに提供することができるが、同じ情報を信頼のないクライアント・コンピュータ・システムには提供することができない。

10

【0066】

サーバ・コンピュータ・システム211は、知らされた機能が適切にサポートされていることを検証するためにブラウザ202をテストする場合がある。例えば、ブラウザ202がgzip圧縮に対するサポートを示す場合、サーバ・コンピュータ・システム211は、ブラウザ202がgzip圧縮コンテンツを適切に処理するか否かを判定するためにgzip圧縮コンテンツをクライアント・コンピュータ・システム201に送信することができる。クライアント・コンピュータ・システム201が、gzip圧縮に対するサポートを指示する適切な要求ヘッダーを構成することがあってよい。クライアント・コンピュータ・システム201は、サーバ・コンピュータ・システム211へ送信され/サーバ・コンピュータ・システム211で受信されるクライアント要求に、適切な要求ヘッダーを含めることができる。これに呼応して、サーバ・コンピュータ・システム211は、クライアント・コンピュータ・システム201がgzip圧縮したコンテンツを適切にキャッシュして、ウェブ・ベースのアプリケーションのセキュリティと保全性(integrity)を害さない方法でgzip圧縮したコンテンツを処理するか否かを判定するために、クライアント・コンピュータ・システムに問い合わせることができる。

20

【0067】

方法500は、選択され、特定された通信プロパティに従って通信フィルタを構成する動作（動作504）を含む。動作504は、サーバ・コンピュータ・システムが、任意の選択された通信プロパティとクライアントがサポートするものであると特定された他の関連プロパティに従ってクライアントとのHTTP通信を処理するよう通信フィルタを構成することを含むことができる。例えば、サーバ・コンピュータ・システム211は、ブラウザ202の通信プロパティ選択（例えば、上級クライアントおよび信頼のないクライアント・コンピュータ・システム）と特定された他の関連通信プロパティ（例えば、HTTP圧縮サポート）に従ってクライアント・コンピュータ・システム201とのHTTP通信を処理するように通信フィルタ243を構成することができる。

30

【0068】

HTTPメッセージがサーバ・コンピュータ・システム211からクライアント・コンピュータ・システム201に送信される場合、通信フィルタ243は、コンテンツがクライアント・コンピュータ・システム201の通信プロパティに準拠するようにHTTPメッセージ・ヘッダーとHTTPメッセージのコンテンツを変更することができる。例えば、電子メール・サーバ212が圧縮されていない電子メール情報を有するメッセージをクライアント・コンピュータ・システム201に送信する場合、通信フィルタ243は、メッセージをインターセプトし、コンテンツをgzip圧縮し、その電子メール情報がgzip圧縮されていることを示すようにメッセージ・ヘッダーを変更することができる。別法として、例えば、インターネット情報サーバ（「IIS」）のモジュールのようなサーバ・コンピュータ・システムの他のモジュールは、gzip圧縮を実装することができる。この結果、コンテンツを、クライアント・コンピュータ・システムの機能を最大限に活用し、ユーザの望みに従うように、クライアント・コンピュータ・システムで提示することができる。

40

50

【0069】

サーバ・コンピュータ・システム211が、クライアント側のブラウザが「プライベート・クライアント・コンピュータ・システム」にあることを指示する選択を受信する場合、ユーザの資格証明書をセキュリティ保護するために、例えばプライベート鍵ストア231のようなプライベート循環鍵ストアを使用することができる。一方、サーバ・コンピュータ・システム211が、クライアント側のブラウザが「信頼のないクライアント・コンピュータ・システム」にあることを指示する選択を受信する場合、ユーザの資格証明書をセキュリティ保護するために、信頼のない鍵ストア221のような信頼のない循環鍵ストアを使用することができる。

【0070】

次に再び図3を参照すると、方法300は、資格証明書をサーバに提出するためにログイン・ページを使用する動作(動作303)を含む。動作303は、クライアント・コンピュータ・システムが、資格証明書をサーバ・コンピュータ・システムに提出するためにログイン・ページを使用することを含むことができる。例えば、クライアント・コンピュータ・システム201は、資格証明書を(場合によっては、通信プロパティ選択と共に)サーバ・コンピュータ・システム211に提出するためにログイン・ページ217を使用することができる。ユーザの資格証明書と通信プロパティ選択を、ログイン要素のフォーマット・バリデータ(format validator)に提出されるポスト・メッセージにログイン要素として含めることができる。例えば、クライアント・コンピュータ・システム201は、ログイン要素273を含むポスト・メッセージ254をサーバ・コンピュータ・システムに送信することができる。

【0071】

方法300は、ログイン・ページで提出されたユーザの資格証明書を受信する動作(動作308)を含む。動作308は、サーバ・コンピュータ・システムが、ログイン・ページで提出されたユーザの資格証明書を受信することを含むことができる。例えば、サーバ・コンピュータ・システム211は、クライアント・コンピュータ・システム201から(場合によっては、通信プロパティ選択と共に)ユーザの資格証明書を受信することができる。資格証明書と通信プロパティ選択は、ポスト・メッセージでログイン要素として受信することができる。例えば、サーバ・コンピュータ・システム211は、ログイン要素273を含むポスト・メッセージ254をクライアント・コンピュータ・システム201から受信することができる。通信フィルタ243を通過する破線を示すように、通信フィルタ243を、ポスト・メッセージ254を変更せずにポスト・メッセージ254を通過させることができるように構成することができる。この結果、ポスト・メッセージ254を、修正なしにログイン要素バリデータ216に転送することができる。その修正の可能性、悪質な処理またはパケットに対するユーザの「スニффイング(sniffing)」を低減し、また媒介者攻撃の可能性を低減するために、例えばトランスポート・レイヤ・セキュリティ(「TLS」)またはセキュア・ソケット・レイヤ(「SSL」)を使用した相互に認証された接続を、適宜、クライアント・コンピュータ・システムとサーバ・コンピュータ・システムの間を設定することができる。

【0072】

ログイン要素バリデータ(検証器)216は、クライアント・コンピュータ・システム201に対する例えばグローバル一意識別子(「GUID」)のような一意識別子を生成することもできる。ログイン要素バリデータ216は、受信したユーザの資格証明書(例えば、ログイン要素273に含まれる)をセキュリティ保護するために、デジタル署名と暗号アルゴリズムを使用することができる。例えば、ログイン要素バリデータ216は、受信したユーザの資格証明書の有効性を引き続いて確認するために使用されるデジタル署名を生成することができる。ログイン要素バリデータ216は、循環鍵ストアの最新の鍵と生成された一意識別子と第1の定数列との組み合わせを(例えば、SHA-1またはMD-5ハッシング・アルゴリズムを使用して)ハッシュすることにより、データにデジタル署名するために使用することのできる署名鍵を導出することができる。いくつかの実施形

10

20

30

40

50

態では、デジタル署名はハッシュ・メッセージ認証コードとして表される。したがって、次の式1によって署名鍵を導出することができる。

$K_{SIG} = SHA-1(K_{MOST_CURRENT_ROTATING_GUID}, HMACKeyString) \dots$ 式1
【0073】

式1で、 $K_{MOST_CURRENT_ROTATING}$ は、適切な循環鍵ストアの最新の鍵を表している。例えば、ブラウザ202が（例えば、通信プロパティ選択によって指示されるように）「プライベート・クライアント・コンピュータ・システム」にある場合、 $K_{MOST_CURRENT_ROTATING}$ はプライベート循環鍵ストア231の最新の鍵（例えば、鍵232）を表す。GUIDは、クライアント・コンピュータ・システム201に対応する一意識別子を表す。HMACKeyStringは、テキストの定数列を表す。次の式2によって K_{SIG} からハッシュ・メッセージ認証コードを生成することができる。

デジタル署名 = $HMAC(K_{SIG}, (GUID, \{ユーザ名: パスワード\}, フラグ)) \dots$ 式2

【0074】

式2で、HMACは、例えばRequest For Comments（「RFC」）2104に記載のようなハッシュ・メッセージ認証コード・アルゴリズムを表す。式2の（GUID、{ユーザ名: パスワード}、フラグ）部分は、GUIDとユーザの資格証明書と通信プロパティ選択がハッシュ・メッセージ認証コード・アルゴリズムに入力されるテキストとして含まれることを表すフラグとを表す。ユーザの資格証明書を、適宜、ハッシュ・メッセージ認証コード・アルゴリズムに準拠させるためにテキスト形式に（例えば、ユーザの資格証明書をbase64符号化することによって）変換することができる。ハッシュ・メッセージ認証コード・アルゴリズムに関して説明したが、デジタル署名を生成するために使用されるアルゴリズムは重要ではなく、事実上いかなるデジタル署名、ダイジェスト、または認証コード・アルゴリズムを使用することもできる。

【0075】

ログイン要素バリデータ216は、循環鍵ストアの最新の鍵と一意識別子と第2の定数列との組み合わせをハッシュすることによって、データを暗号化するために使用することのできる暗号鍵を導出することもできる。したがって、次の式3によって暗号鍵を導出することができる。

$K_{ENC} = SHA-1(K_{MOST_CURRENT_ROTATING_GUID}, EncryptKeyString) \dots$ 式3

【0076】

式3で、 $K_{MOST_CURRENT_ROTATING}$ は、署名鍵を生成する際に使用された循環鍵ストアからの最新の鍵を表す。したがって、 K_{SIG} を生成するために鍵232が使用された場合、鍵232は K_{ENC} を生成するためにも使用することができる。GUIDは、クライアント・コンピュータ・システム201に対応する一意識別子を表す。EncryptKeyStringは、HMACKeyStringとは異なるテキストの定数列を表す。したがって、次の式4によって暗号化された情報を生成することができる。

暗号化された情報 = $K_{ENC} [デジタル署名, \{ユーザ名: パスワード\}, フラグ] \dots$ 式4

【0077】

式4では、デジタル署名は、式2によって生成されたデジタル署名を表し、{ユーザ名: パスワード}はユーザの資格証明書を表し、フラグは通信プロパティ選択を表す。

【0078】

ステップ311は、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号化された情報を送信する対応する動作（動作309）を含む。動作309は、サーバ・コンピュータ・システムが、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号

10

20

30

40

50

化された情報をクライアント・コンピュータ・システムに送信することを含むことができる。例えば、ログイン要素バリデータ216は、GUID274および暗号化された資格証明書275を含むメッセージ255をクライアント・コンピュータ・システム201に送信することができる。通信フィルタ243を通過する縦線を示すように、通信フィルタ243を、メッセージ255を変更せずに通過させるように構成することができる。したがって、メッセージ255を修正なしにクライアント・コンピュータ・システム201に転送することができる。

【0079】

方法300は、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号化された情報を受信する動作(動作304)を含む。動作304は、クライアント・コンピュータ・システムが、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号化された情報をサーバ・コンピュータ・システムから受信することを含むことができる。例えば、クライアント・コンピュータ・システム201は、GUID274と暗号化された資格証明書275を含むメッセージ255をサーバ・コンピュータ・システム211から受信することができる。クライアント・コンピュータ・システム201がGUID274と暗号化された資格証明書275をクッキー203に記憶するように、メッセージ255を構成することができる。例えば、メッセージ255は次のように構成することができる。

Set-Cookie: sessionid = {GUID}; パス= /

Set-Cookie: creddata = {暗号化された情報}; パス= /

【0080】

方法300は、暗号化された情報を含む第2の要求を送信する動作(動作305)を含む。動作305は、クライアント・コンピュータ・システムが、リソース(例えば、第1の要求で要求された電子メール・メッセージ)へのウェブ・ベースのアクセスを求める第2の要求を送信することを含むことができる。例えば、クライアント・コンピュータ・システム201は、メール・サーバのURI267とGUID274と暗号化された資格証明書275を含む要求256をサーバ・コンピュータ・システム211に送信することができる。方法300は、暗号化された情報を受信する動作(動作310)を含む。動作310は、サーバ・コンピュータ・システムが、リソース(例えば、第1の要求で要求された電子メール・メッセージ)へのウェブ・ベースのアクセスを求める第2の要求を受信することを含むことができる。例えば、サーバ・コンピュータ・システム211は、メール・サーバのURI267とGUID274と暗号化された資格証明書275を含む要求256をクライアント・コンピュータ・システム201から受信することができる。

【0081】

いくつかの実施形態では、クライアント・コンピュータ・システムは、GUIDと暗号化された情報を有する対応するクッキーをブラウザ・メモリに既に記憶している。この記憶されているGUIDと暗号化された情報とを、サーバのリソース(例えば、電子メールのデータ)へのウェブ・ベースのアクセスを要求する場合に、使用することができる。図2Bは、本発明により、サーバのリソースにアクセスするためにセキュリティ保護されたクライアント側の資格証明書を使用することに役立つネットワーク・アーキテクチャ200の一例を示している。図4は、本発明による、セキュリティ保護されたクライアント側の資格証明書をサーバのリソースへのアクセスに使用することを容易にする方法400の流れ図の一例を示している。方法400を、図2Bに示すクライアント・コンピュータ・システムとサーバ・コンピュータ・システムに関して説明する。

【0082】

図400は、サーバのリソースへのウェブ・ベースのアクセスを求める、セッションIDと暗号化されたユーザの資格証明書を含む、要求を送信する動作(動作401)を含む。動作401は、クライアント・コンピュータ・システムが、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を送信することを含むことができる。例えば、クライアント・コンピュータ・システム201は、メール・サーバの

10

20

30

40

50

URI 267とGUID 274と暗号化された資格証明書275とを含む要求(リクエスト) 291をサーバ・コンピュータ・システム211に送信することができる。メール・サーバのURI 267は、電子メール・サーバ212によって制御されている電子メール・リソースへのアクセスを提供するURIを表す。GUID 274は、以前にサーバ・コンピュータ・システム211からクライアント・コンピュータ・システム201に送信された一意のセッションIDを表す。暗号化された資格証明書275は、以前にサーバ・コンピュータ・システム211からクライアント・コンピュータ・システム201に送信された暗号化されたユーザの資格証明書と時間依存署名とを表す。暗号化された資格証明書275は、適切な循環鍵ストアの鍵から既に生成済みである。

【0083】

方法400は、サーバのリソースへのウェブ・ベースのアクセスを求める、セッションIDと暗号化されたユーザの資格証明書とを含む要求を受信する動作(動作404)を含む。動作404は、サーバ・コンピュータ・システムが、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を受信することを含むことができる。例えば、サーバ・コンピュータ・システム211は、メール・サーバのURI 267とGUID 274と暗号化された資格証明書275とを含む要求291をクライアント・コンピュータ・システム201から受信することができる。

【0084】

方法400は、循環鍵ストアの最新の鍵を使用して暗号化されたユーザの資格証明書の有効性確認を試みる動作(動作405)を含む。動作405は、サーバ・コンピュータ・システムが、循環鍵ストアの最新の鍵を使用してユーザの資格証明書の少なくとも一部の有効性確認を試みることを含むことができる。例えば、ブラウザ202がプライベート・クライアント・コンピュータ・システムにあることが示された場合、サーバ・コンピュータ・システムは鍵232を使用して暗号化された資格証明書275の有効性確認を試みる。一方、ブラウザ202が信頼のないクライアント・コンピュータ・システムにあることが示された場合、サーバ・コンピュータ・システムは、鍵222を使用して暗号化された資格証明書275の有効性確認を試みることができる。資格証明書バリデータ237は、適切な循環鍵ストアの最新の鍵と一意識別子と第2の定数列(暗号鍵を導出する際に使用される)との組み合わせをハッシュすることによって、データを暗号解読するために使用される暗号解読鍵を導出することができる。したがって、次の式5によって暗号解読鍵を導出することができる。

$$K_{DCR} = \text{SHA-1}(K_{\text{MOST CURRENT ROTATING}}, \text{GUID}, \text{EncryptKeyString}) \cdots \text{式5}$$

【0085】

式5では、 $K_{\text{MOST CURRENT ROTATING}}$ は適切な循環鍵ストアの最新の鍵(例えば、鍵232または鍵222)を表す。GUIDは、クライアント・コンピュータ・システム201に対応する一意識別子を表す。EncryptKeyStringは、 K_{ENC} の導出中に使用される定数列を表す。したがって、資格証明書バリデータ237は、次の式6によって、デジタル署名とユーザの資格証明書と通信プロパティ選択を表すフラグとを明らかにするために暗号化された情報を暗号解読することができ。

$$\text{デジタル署名}, \{\text{ユーザ名:パスワード}\}, \text{フラグ} = K_{DCR} [\text{暗号化された情報}] \cdots \text{式6}$$

【0086】

資格証明書バリデータ237は、適切な循環鍵ストアの最新の鍵と一意識別子と第1の定数列との組み合わせをハッシュすることによって、有効性確認デジタル署名を生成するために使用することができる有効性確認鍵を導出することができる。いくつかの実施形態では、有効性確認デジタル署名はハッシュ・メッセージ認証コードとして表される。したがって、次の式7によって有効性確認鍵を導出することができる。

$$K_{VAL} = \text{SHA-1}(K_{\text{MOST CURRENT ROTATING}}, \text{GUID}, \text{HMACKeyString}) \cdots \text{式7}$$

10

20

30

40

50

【0087】

式7では、 $K_{MOST\ CURRENT\ ROTATING}$ は、適切な循環鍵ストアの最新の鍵を表す。GUIDは、クライアント・コンピュータ・システム201に対応する一意識別子を表す。HMACKeyStringは、署名鍵を導出する場合に使用されるテキストの定数列を表す。KVALから、また式6から明らかになったユーザの資格証明書とフラグを使用して、ハッシュ・メッセージ認証コードを次の式8によって生成することができる。

有効性確認デジタル署名 = $HMAC(KVAL, (GUID, \{ユーザ名: パスワード\}, フラグ)) \cdots$ 式8

【0088】

式8では、HMACはハッシュ・メッセージ認証コード・アルゴリズムを表す。式8の(GUID、{ユーザ名: パスワード}、フラグ)の部分は、GUIDとユーザの資格証明書と通信プロパティ選択を表すフラグがハッシュ・メッセージ認証コード・アルゴリズムに入力されるテキストとして含まれていることを表す。ハッシュ・メッセージ認証コード・アルゴリズムに関して説明しているが、有効性確認デジタル署名を生成するために使用されるこのアルゴリズムは重要ではなく、事実上いかなるデジタル署名、ダイジェスト、または認証コード・アルゴリズムでも使用することができる。

【0089】

有効性確認デジタル署名がデジタル署名と等しい場合、暗号化された資格証明書275で表されたユーザの資格証明書は有効であるとされる。したがって、通信フィルタ243は、有効であるとされたユーザの資格証明書を含む許可ヘッダー（例えば、HTTP許可ヘッダー）を構築する。通信フィルタ243は、リソースへのウェブ・ベースのアクセスを求める要求に許可ヘッダーを挿入することができる。例えば、通信フィルタ243は、要求291から暗号化された資格証明書275を除去し、要求291に資格証明書289を挿入することができ、この結果、要求291Aが生じる。

【0090】

有効性確認デジタル署名がデジタル署名に等しくない場合、ユーザの資格証明書は有効であるとされない。したがって、資格証明書バリデータ237は、適切な循環鍵ストアの次に新しい鍵に基づいて式5、6、7および8の機能を反復する。例えば、プライベート・クライアント・コンピュータ・システムのクライアント側のブラウザに対して、資格証明書バリデータ237は鍵233を使用することができる。一方、信頼のないクライアントのクライアント側のブラウザに対しては、資格証明書バリデータ237は鍵223を使用することができる。資格証明書バリデータは、適切な循環鍵ストアの各鍵を使用してユーザの資格証明書の有効性確認を試みることができる。有効であるとされたユーザの資格証明書は、適切な認証ヘッダーに含めることができる。

【0091】

いくつかの実施形態では、暗号化された資格証明書の有効性確認を試みるために使用されるべき循環鍵（例えば、資格証明書を暗号化するために以前使用された循環）を指示するために、インデックスが、暗号化された資格証明書と共に含まれる。例えば、クライアント・コンピュータ・システム201は、信頼のない循環鍵ストア221またはプライベート循環鍵ストア231の循環鍵を特定するインデックスを、要求291に含めることができる。インデックスは、使用されるべき循環鍵の生成を特定する数値（例えば、0、1、2など）であってよい。例えば、クライアント・コンピュータ・システム201がプライベート・クライアント・コンピュータ・システムである場合、インデックス0は鍵232を特定することができる。同様に、クライアント・コンピュータ・システム201が信頼のないクライアント・コンピュータ・システムである場合、インデックス2は鍵224を特定することができる。したがって、インデックスを使用することによって有効性確認プロセスの効率が高まる。資格証明書がインデックスで特定された循環鍵によって有効であるとされない場合、対応する循環鍵ストアの他の鍵を使用して資格証明書の有効性確認を試みることができる。

10

20

30

40

50

【0092】

方法400は、要求されたリソースへのウェブ・ベースのアクセスを制御するモジュールに要求を転送する動作（動作406）を含む。動作406は、サーバ・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを制御するモジュールに要求を転送することを含むことができる。例えば、通信フィルタ243は、（暗号化された資格証明書275から明らかになるような）メール・サーバのURL267と資格証明書289とを含む要求291Aを電子メール・サーバ212に転送することができる。電子メール・サーバ212は、電子メール・リソースへのウェブ・ベースのアクセスを制御するモジュールであってよい。電子メール・サーバ212は、要求された電子メール・リソースへのウェブ・ベースのアクセスが許可されているか否かを判定するために資格証明書289を資格証明書データベース213と比較することができる。

10

【0093】

方法400は、リフレッシュされた暗号化されたユーザの資格証明書を循環鍵ストアの最新の鍵から導出すべきか否かを判定する動作（動作407）を含む。動作407は、サーバ・コンピュータ・システムが、ユーザの資格証明書と時間依存署名を表すリフレッシュされた暗号化された情報を循環鍵ストアの最新の鍵から導出すべきか否かを判定することを含むことができる。ユーザの資格証明書が循環鍵ストアの最新の鍵以外の鍵によって有効であるとされる場合、サーバはリフレッシュされた暗号化された情報が導出されるべきであると決定する。例えば、資格証明書バリエータ237が暗号化された資格証明書を鍵224によって有効であるとする場合、通信フィルタ243は、暗号化された資格証明書に表されたユーザの資格証明書に関して、リフレッシュされた暗号化された資格証明書が導出されるべきであると決定することができる。

20

【0094】

したがって、破線で示したように、通信フィルタ243は、要素バリエータ216にログインするために任意選択でクッキー・リフレッシュ要求294を送信することができる。ログイン要素バリエータ216は、（例えば、最新の鍵からリフレッシュされたデジタル署名とリフレッシュされた暗号鍵を導出することによって）リフレッシュされた暗号化された情報を導出するために適切な循環鍵ストアの最新の鍵を使用することができる。ログイン要素バリエータ216は、更新されたGUIDとリフレッシュされた暗号化された資格証明書とを通信フィルタ243に返信することができる。例えば、破線で示すように、ログイン要素バリエータ216は、更新されたGUID296とリフレッシュされた暗号化された資格証明書297を含むメッセージ295を通信フィルタ243に返信する。

30

【0095】

資格証明書289が、電子メール・サーバ212の電子メール・リソースへのウェブ・ベースのアクセスに適切である場合、電子メール・サーバ212は、要求291Aに呼応して電子メール・リソースを返信することができる。例えば、電子メール・サーバ212は、リソース293（例えば、電子メール・メッセージ）を含む応答（レスポンス）292を通信フィルタ243に返信することができる。一方、資格証明書289が、電子メール・サーバ212の電子メール・リソースへのウェブ・ベースのアクセスに適切でない場合、電子メール・サーバ212は、要求291Aに呼応して無許可であるという指示を返信することができる。例えば破線で示すように、電子メール・サーバ212は、無許可インジケータ272を含む応答（レスポンス）294を通信フィルタ243に返信することができる。通信フィルタ243が無許可インジケータを受信する場合、通信フィルタ243はクライアント・コンピュータ・システム201をログイン・ページ217にリダイレクトすることができる。

40

【0096】

有効性確認されたユーザの資格証明書が適切である場合、通信フィルタ243は要求されたリソースをクライアント・コンピュータ・システム201に送信することができる。例えば、暗号化された資格証明書275が適切な循環鍵ストアからの最新の鍵によって有効性確認される場合、リソース293を含む応答292は通信フィルタ243で受信され

50

る。通信フィルタ 243 は、応答 292 をクライアント・コンピュータ・システム 201 に転送することができる。したがって、リソース 293 がブラウザ 202 で提示される。

【0097】

有効性確認されたユーザの資格証明書が適切である場合、通信フィルタ 243 は、リフレッシュされた暗号化された資格証明書と更新された G U I D もリソースと共にクライアント・コンピュータ・システム 201 に送信することができる。例えば、暗号化された資格証明書 275 が循環鍵ストアの最新の鍵ではない鍵によって有効性確認される場合、リソース 293 と更新された G U I D 296 とリフレッシュされた暗号化された資格証明書 297 をすべて通信フィルタ 243 で受信することができる。破線で示すように、次いで通信モジュール 243 は、リソース 293 と更新された G U I D 296 とリフレッシュされた暗号化された資格証明書 297 とを含む応答 (レスポンス) 276 をクライアント・コンピュータ・システム 201 に送信することができる。

【0098】

方法 400 は、リソースを、更新されたセッション ID とリフレッシュされた暗号化されたユーザの資格証明書と共に、クライアント側のブラウザで受信する動作 (動作 402) を含む。動作 402 は、クライアント・コンピュータ・システムが、要求されたものを、更新されたセッション ID と、ユーザの資格証明書の少なくとも一部とリフレッシュされた時間依存署名を表すリフレッシュされた暗号化された情報と共に、受信することを含むことができる。例えば、クライアント・コンピュータ・システム 201 は、リソース 293 と更新された G U I D 296 とリフレッシュされた暗号化された資格証明書 297 とを含む応答 276 をサーバ・コンピュータ・システム 201 から受信することができる。

【0099】

方法 400 は、更新されたセッション ID とリフレッシュされた暗号化されたユーザの資格証明書を対応するクッキーに記憶する動作 (動作 403) を含む。動作 403 は、クライアント・コンピュータ・システムが、更新されたセッション ID とリフレッシュされた暗号化された情報をクライアント・コンピュータ・システムの対応するクッキーに記憶することを含むことができる。例えば、更新された G U I D 296 とリフレッシュされた暗号化された資格証明書 297 で G U I D 274 と暗号化された資格証明書 275 を上書きして、クッキー 203 の対応するクッキーに記憶することができる。

【0100】

本発明は、その趣旨または本質的な特性から逸脱せずに他の特定の形式で実施することができる。記載した実施形態は、すべての点で説明のみを目的としたものであり限定を目的としたものではないとみなされるべきである。したがって、本発明の範囲は上記の説明ではなく特許請求の範囲によって示される。特許請求の範囲と等価の意味および範囲内のすべての変異は、本特許請求の範囲に包含されるべきである。

【図面の簡単な説明】

【0101】

【図 1】本発明の原理に適した動作環境を示す図である。

【図 2 A】本発明による、クライアントがサーバのリソースへのアクセスを要求する場合にクライアント側の資格証明書をセキュリティ保護することに役立つネットワーク・アーキテクチャの一例を示す図である。

【図 2 B】本発明による、サーバのリソースにアクセスするためにセキュリティ保護されたクライアント側の資格証明書を使用することに役立つネットワーク・アーキテクチャの一例を示す図である。

【図 3】本発明による、クライアントがサーバのリソースへのアクセスを要求する場合にクライアント側の資格証明書をセキュリティ保護する方法の流れ図の一例を示す図である。

【図 4】本発明による、サーバのリソースにアクセスするためにセキュリティ保護されたクライアント側の資格証明書を使用する方法の流れ図の一例を示す図である。

【図 5】本発明の原理による、クライアントに関連付けられた通信プロパティを決定する

10

20

30

40

50

方法の流れ図の一例を示す図である。

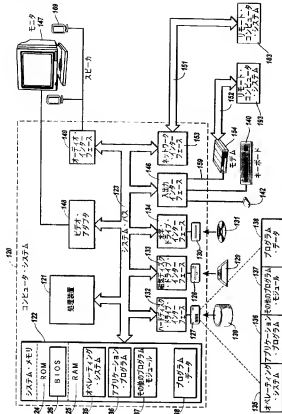
【図6】本発明の原理による、資格証明書と通信プロパティ選択を受諾することができるログイン・ページの一例を示す図である。

【符号の説明】

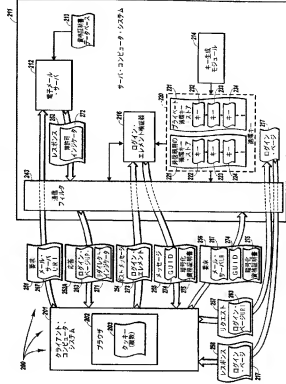
【0102】

120	コンピュータ・システム	
121	処理装置	
122	システム・メモリ	
123	システム・バス	
132	ハードディスク・ドライブ・インターフェース	10
133	磁気ディスクドライブ・インターフェース	
134	光ディスク・インターフェース	
135	オペレーティング・システム	
136	アプリケーション・プログラム	
137	他のプログラム・モジュール	
138	プログラム・データ	
140	キーボード	
146	入出力インターフェース	
147	モニタ	
148	ビデオ・アダプタ	20
149	音声インターフェース	
153	ネットワーク・インターフェース	
154	モデム	
169	スピーカ	
183	遠隔コンピュータ・システム	
193	遠隔コンピュータ・システム	

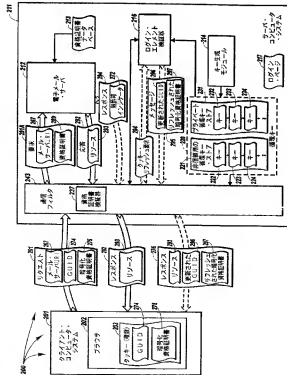
【図 1】



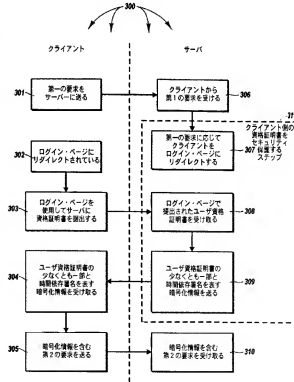
【図 2 A】



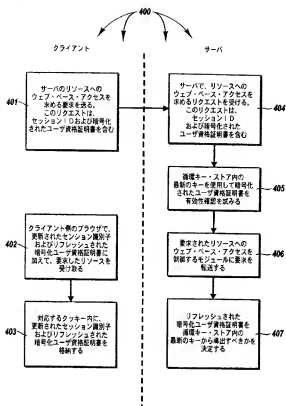
【図 2 B】



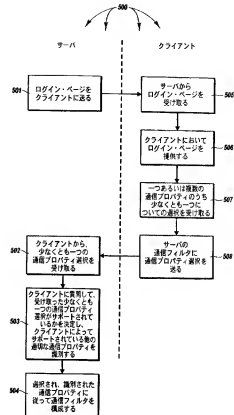
【図 3】



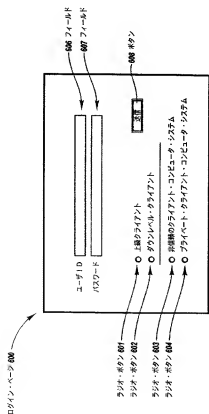
【図 4】



【図 5】



【図 6】



 フロントページの続き

- (72)発明者 リチャード ビー. ウォード
 アメリカ合衆国 98053 ワシントン州 レッドモンド 261 アベニュー ノースイースト 8565
- (72)発明者 ラッセル リー シンプソン ジュニア
 アメリカ合衆国 98034 ワシントン州 カークランド 79 プレイス ノースイースト 11136
- (72)発明者 カリム ミシェル パティシュ
 アメリカ合衆国 98117 ワシントン州 シアトル メイビー アベニュー ノースウエスト 9214
- F ターム(参考) 5B085 AE02 AE03 AE09 BC01
 5J104 AA07 AA16 AA34 EA04 EA19 JA21 KA01 KA04 LA03 NA02
 NA05 NA12 NA37 NA38 PA07

【要約の続き】

PAT-NO: JP02004173285A
DOCUMENT-IDENTIFIER: JP 2004173285 A
TITLE: SECURE PROCESSING OF CLIENT
CREDENTIALS USED FOR WEB-
BASED ACCESS TO RESOURCE
PUBN-DATE: June 17, 2004

INVENTOR-INFORMATION:

NAME	COUNTRY
BRACEWELL, SHAWN DEREK	N/A
WARD, RICHARD B	N/A
SIMPSON, RUSSELL LEE JR	N/A
BATTHISH, KARIM MICHEL	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
MICROSOFT CORP	N/A

APPL-NO: JP2003391491
APPL-DATE: November 20, 2003

PRIORITY-DATA: 2002428152 (November 20, 2002) ,
2003459863 (June 12, 2003)

INT-CL (IPC): H04L009/32 , G06F015/00 ,
G09C001/00 , H04L009/16

ABSTRACT:

PROBLEM TO BE SOLVED: To provide secure processing of client credentials used for Web-based access to resources.

SOLUTION: A login page with an interface for entering user credentials is presented at a client and the entered user credentials are sent to a server. In response to receiving the user credentials, the server generates a unique session ID for the client. The server also derives a digital signature for the user credentials based on a current key in a rotating key store and the unique session ID. The server then encrypts the digital signature and the user credentials based on an encryption key derived from the current key and the unique session ID. When encrypted credentials are received back to the client, keys from the rotating key store are used to attempt to validate the credentials. If the user credentials can not be validated, a user is again presented with a login page.

COPYRIGHT: (C) 2004, JPO